User Guide

Linksys E1550 | Wireless-N Router with SpeedBoost

Contents

Product overview

Setting Up: Basics

Setting Up: Advanced

Improving Security

Port Forwarding and Port Triggering

Maintaining and Monitoring

Specifications

Browser-based Utility Menu Structure

Product overview

Package contents

In addition to your router, your router package includes:

- Network (Ethernet) cable
- AC power adapter
- Setup CD containing router setup software and documentation

Features

Wireless-N technology

Built with leading 802.11n wireless technology, your router offers maximum speed and range to create an ultra-powerful network designed for home theater performance. Connect your computers, Internet-ready TVs, game consoles, smartphones and other Wi-Fi devices at blazingly fast transfer rates for an unrivaled experience.

SpeedBoost

Higher quality antenna technology helps maintain high speeds across greater distances throughout your home.

State-of-the-art security

Keep Wi-Fi freeloaders and Internet threats at bay with WPA/WPA2 encryption. An SPI firewall helps keep your network protected.

Benefits of Fast Ethernet

Use the four Fast Ethernet (10/100) ports for quick file sharing between computers and servers.

Built-in USB port

The USB storage port lets you add an external USB drive to your network and share files at home or over the Internet.

Home network ready

Connect computers, printers, and more to your wireless network and the Internet. QoS traffic prioritization technology delivers maximum speed and performance so you can enjoy fast downloads and reliable gaming.

Easy to manage

Cisco Connect software helps you customize your settings and quickly add multiple devices to your network:

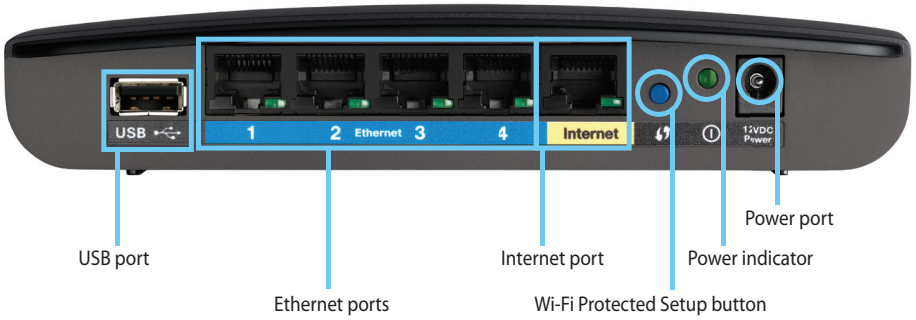
Separate guest network

Create a separate, secure, password-protected network for guests.

Parental controls

Limit access time and websites with parental controls.

Back view

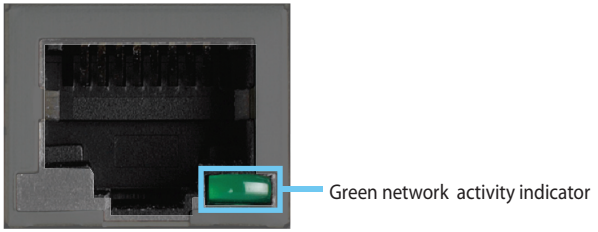


- **USB port**— To easily share disk storage with other users on your network or on the Internet, connect a USB drive to this port. For more information, see "Using an External Drive" on page 32.
- **Ethernet ports**—Connect Ethernet cables (also called network cables) to these Fast Ethernet (10/100) ports, color coded blue, and to other wired Ethernet network devices on your network.
- **Internet port**—Connect an Ethernet cable (also called a network or Internet cable) to this port, color coded yellow, and to your modem.

  Wi-Fi Protected Setup™ button—Press this button to easily configure wireless security on Wi-Fi Protected Setup-enabled network devices. For more information, see "How to set up wireless security using Wi-Fi Protected Setup" on page 28.
- **Power indicator**—Stays on steadily while power is connected and following a successful Wi-Fi Protected Setup connection. Flashes slowly during bootup, during firmware upgrades, and during a Wi-Fi Protected Setup connection. Flashes quickly when there is a Wi-Fi Protected Setup error.
- **Power**—Connect the included AC power adapter to this port.

CAUTION
Use only the adapter that came with your router.

Port activity indicator



Network and Internet port

- **Green activity indicator**—On Ethernet ports, stays on when a cable connects the port to another Ethernet port. On the Internet port, stays on while connected to a modem. On both port types, it flashes while transferring data.

Bottom view

- **Reset button**—Press and hold this button for 5-10 seconds (until the port lights flash at the same time) to reset the router to its factory defaults. You can also restore the defaults using the browser-based utility. For more information, see "How to restore factory defaults" on page 43.

Setting Up: Basics

How to create a home network

What is a network?

A network is any group of devices that can communicate with each other. A home network can also include Internet access, which requires a router like this one.

A typical home network may include multiple computers, a printer, a modem, and a router. A large home network may also have a switch, additional routers, access points, and many Internet-capable media devices such as TVs, game consoles, and web cameras.

- **Modem**—Connects a computer or a router to your ISP (Internet Service Provider).
- **Router**—Connects your wireless and wired network devices to each other and to the modem (and to your ISP).
- **Switch**—Allows you to connect several wired network devices to your home network. Your router has a built-in network switch (the Ethernet ports). If you have more wired network devices than available Ethernet ports on your router, you will need an additional switch to consolidate the wired connections.

How to set up a home network

1. Purchase the proper equipment. For a network that includes Internet access, you'll need:
   - Computers with an Ethernet port or wireless networking capabilities
   - A modem for connecting to your ISP (typically supplied by your ISP)
   - A router to connect your computers with each other and to the modem
   - Internet service to your home, provided by an ISP (Internet Service Provider)
2. Make sure that your modem is working. Your ISP can help you set up your modem and verify that it's working correctly.
3. Set up your router. See "How to set up your router" on page 3.
4. To connect a computer or other network device to the network, see "How to connect a computer to your network" on page 6 and "How to connect other devices" on page 8.

Where to find more help

In addition to this User Guide, you can find help at these locations:

- **Linksys.com/support** (documentation, downloads, FAQs, technical support, live chat, forums)
- Setup CD (Troubleshooting Guide, legal and regulatory notices)
- Cisco Connect help (run Cisco Connect, then click Learn More where available)
- Browser-based utility context-sensitive help (open the utility, then click **Help** in the right-side column.)

How to set up your router

The easiest and fastest way to set up your router is to run the Cisco Connect setup software. You can find Cisco Connect on the CD that came with your router or download it from the router's support site at Linksys.com/support. Cisco Connect shows you how to connect your router to your home network, step by step. To get started, see "How to start Cisco Connect" below.

If you are an advanced user, you can set up your router manually using the browser-based utility. To get started, see "How to open the browser-based utility" on page 14.

How to start Cisco Connect

When you run the setup CD, Cisco Connect (your router's setup software) is automatically installed onto your computer. You can then use Cisco Connect to easily manage your router. To install Cisco Connect on another computer after your router has been set up, see "How to install Cisco Connect on another computer" on page 5.

NOTES:

Your Cisco Connect CD works with only this router model.

If you lose your setup CD, you can download the software from **Linksys.com/support**.

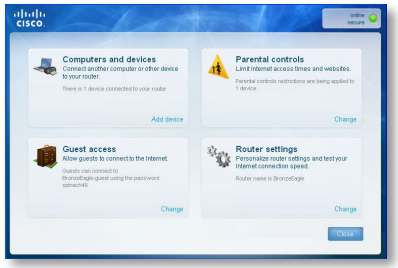
To start Cisco Connect for the first time:

1. Insert the CD into your CD or DVD drive.
2. Click **Set up your Linksys Router**.

   If you do not see this:

   - For Windows, click **Start**, **Computer**, then double-click the **CD** drive and the **Setup** icon.
   - For Mac, double-click the **CD** icon on your desktop, then double-click the **Setup** icon.
3. Follow the on-screen instructions to complete your router setup. When setup has finished, Cisco Connect has also been installed onto your hard drive.

After your router has been set up and Cisco Connect has been installed, you can use Cisco Connect to easily manage many of your router's settings.



To start Cisco Connect on a Windows computer:

1. Click **Start**, **All Programs**, then click **Cisco Connect**. The Cisco Connect main menu opens.

To start Cisco Connect on a Mac OS X computer:

1. Open the **Applications** folder, then double-click the **Cisco Connect** icon. The Cisco Connect main menu opens.

How to install Cisco Connect on another computer

Although Cisco Connect is installed onto your computer when you run the setup CD, you may want to manage your router from a different computer on your network.

> **CAUTION**
> After your router has been set up, do not run the setup CD to install Cisco Connect to another computer. If you run the setup CD again, you will be prompted to enter the router's network name (SSID) and password.

To install Cisco Connect onto another computer:

1. See "How to connect a computer using an Easy Setup Key" on page 6. When finished, Cisco Connect has also been installed onto the computer's hard drive.

How to improve your wireless connection speed

Follow these tips to improve your network's wireless connection speed:

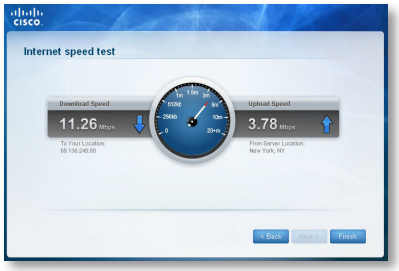
- Make sure that your router is in a good location.
- For the widest coverage area, install your router near the center of your home, and near the ceiling, if possible.
- Avoid placing the router on or near metal objects (such as file cabinets and metal furniture), reflective surfaces (such as glass or mirrors), or masonry walls.
- Any obstruction can weaken the wireless signal (even non-metallic objects), so the fewer obstructions between the router and the wireless device, the better.
- Place the router in a location away from other electronics, motors, and fluorescent lighting.
- Many environmental variables can affect the router's performance, so if your wireless signal is weak, place the router in several locations and test the signal strength to determine the ideal position.
- If possible, upgrade wireless network interfaces (such as wireless network cards in computers) from older wireless standards to 802.11n. If a wirelessly networked device uses an older standard, the performance of the entire wireless network may be slower.

How to test your Internet connection speed

To test your Internet connection speed:

1. Run Cisco Connect, then click **Change** under *Router settings*. The *Router settings* screen opens.

2. Click **Launch Test** under *Internet Speed*. The *Internet speed test* screen opens.
3. Follow the on-screen instructions to complete the test.



How to connect devices to your network

How to connect a computer to your network

You can connect a computer to your network using an Easy Setup Key (the easiest way) or manually.

How to connect a computer using an Easy Setup Key

To use an Easy Setup Key, you first need to create one using any available USB drive. After it has been created, you can use the same key to connect several computers to your network.

> **TIP**
> The Easy Setup Key stores network information (name, password, security type, and security key) so you don't have to remember them.

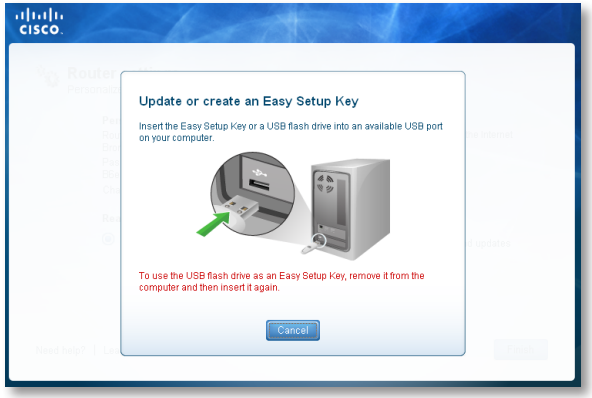
To create an Easy Setup Key:

1. Run Cisco Connect, then click **Add device** under *Computers and devices*. The *Computers and other devices* screen opens.

2. Click **Computer**.

3. Select **No, I don't have an Easy Setup Key**, then click **Next**.
4. Insert a USB drive into an available USB port on your computer. This USB drive will be your new Easy Setup Key.

   Cisco Connect detects the newly attached USB drive and copies the router's settings and a copy of Cisco Connect to it.



5. When the files have finished copying, remove the Easy Setup Key from your computer. You can now use it to install Cisco Connect onto other computers and to connect them to the network.
6. Click **Close**.

To use your Easy Setup Key to connect a computer to your network:

1. Run Cisco Connect, then click **Add device** under *Computers and devices.* The *Computers and other devices* screen opens.
2. Click **Computer**.

3. Select **Yes, I have an Easy Setup Key**, then click **Next**. The *Connecting another computer* screen opens.
4. Insert the Easy Setup Key into an available USB port on the computer that you want to connect to the network. The *Connecting another computer* screen opens.

   If you do not see this, use Windows Explorer or Finder to view the Easy Setup Key files, then double-click **Connect**.
5. Click **Connect to your router**, then follow the on-screen instructions.
6. Return to the computer running Cisco Connect, then click **Next**.
7. Enter a name for the newly connected computer, then click **Finish**.

How to connect a computer manually

To connect a computer without using an Easy Setup Key, you will need to print or take note of some information.

> **IMPORTANT**
> When you manually connect a computer to the network, the computer will *not* have Cisco Connect installed on it.

To manually connect a computer to your network:

1. Run Cisco Connect, then click **Add device** under *Computers and devices.* The *Computers and other devices* screen opens.

2. Click **Computer**.
3. Select **I want to connect manually using my wireless settings**, then click **Next**. A screen opens that displays network information.
4. Write down the Network name (SSID), Security Key, and Security Type information, or click **Print these settings** if you have a printer attached.
5. At the computer you want to connect, enter the network information into your wireless manager.
6. After that computer connects to your network, return to the computer running Cisco Connect, then click **Next**.
7. Click **Connect to your Linksys router**, then follow the on-screen instructions.
8. When you are prompted to enter a name for the newly connected computer, enter the name, then click **Finish**.

How to connect a printer

When you install a printer that requires a cable, follow the printer's instructions for setting it up, then follow your computer's operating system instructions to share the printer with your network.

When you set up a wireless printer, however, it needs to communicate with your router. Before you try to set up your wireless printer, make sure that:

- Your printer has been completely set up except for being connected to the network.
- Your printer supports the WPA/WPA2 wireless encryption standard.
- If your wireless printer supports WPS (Wi-Fi Protected Setup), you should use WPS to connect it to your network. See "How to set up wireless security using Wi-Fi Protected Setup" on page 28.

To connect a wireless printer to your network:

1. Run Cisco Connect, then click **Add device** under *Computers and devices*. The *Computers and other devices* screen opens.

2. Click **Wireless printer**. A screen opens that displays network information.
3. Write down the Network name (SSID), Security Key, and Security Type information, or click **Print these settings** if you have a different printer already connected.
4. Follow your printer's instructions for entering the wireless network information into your printer.
5. After the printer connects to your network, click **Next** in Cisco Connect.
6. Return to the computer running Cisco Connect, then click **Next**. The *Name your printer* screen opens.
7. Enter a name for the printer, then click **Finish**.
8. Follow your computer operating system's instructions for adding the new printer to your list of available printers.

How to connect other devices

Many other types of wireless network devices can connect to your home network, including:

- Game consoles
- Internet-capable TVs and media players
- Digital music players
- Smart phones

Because of the wide variety of devices and methods of connecting, you must manually enter network information into the devices for a successful network connection.

To manually connect a device to your network:

1. Run Cisco Connect, then click **Add device** under *Computers and devices*. The *Computers and other devices* screen opens.

2. Click **Other devices**. A screen opens that displays network information.

3. Write down the Network name (SSID), Security Key, and Security Type information, or click **Print these settings** if you have a printer attached.

4. Follow your device's instructions for entering the wireless network information into the device.
5. After the device connects to your network, return to the computer running Cisco Connect, then click **Next**.
6. Enter a name for device, then click **Finish**.

For more instructions on connecting a game console to your network, see also:

- "How to optimize your router for gaming and voice" on page 19
- "How to set up port forwarding" on page 39
- "How to set up port range triggering for online gaming" on page 41

How to set up parental controls

With your router, you can use parental controls to:

- Set the times that Internet access is allowed.
- Block websites based on their content.
- Block websites that you specify.
- Set the above restrictions for specific computers.

TIP
When someone tries to open a blocked website, a window opens asking for the parental controls password. Enter the password to view the blocked content.

How to access parental controls

The first time you try to access parental controls, you are asked to set a password.

To access parental controls for the first time:

1. Run Cisco Connect, then click **Change** under **Parental controls**. The *Parental controls password* screen opens.

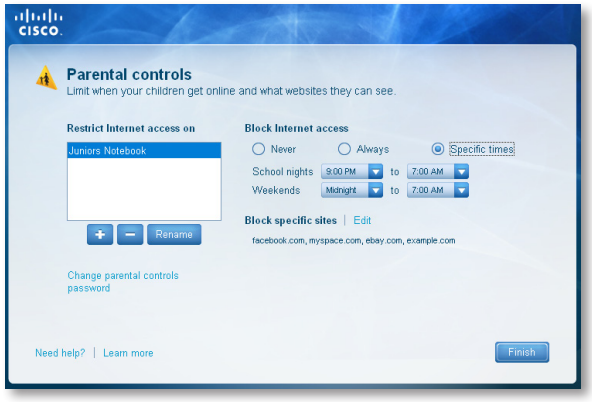
2. Enter a password (from 4 to 32 characters), then enter a secret question and answer.
   - The password must contain from 4 to 32 valid characters, which are A-Z, a-z, and 0-9.
   - The answer to the secret question should be something not easily guessed by others. If you forget your password, you can reset it by correctly answering your secret question.
3. To save your settings, click **OK**. The *Parental controls* main screen appears.

To access parental controls after the first time:

1. Run Cisco Connect, then click **Change** under **Parental controls**. The *Enter the parental controls password* screen opens.
2. Enter the parental control password, then click **OK**.

NOTE
If you forgot the password, click **I forgot my password** and enter the answer to your secret question.

The *Parental controls* main screen appears.



To change the parental controls password:

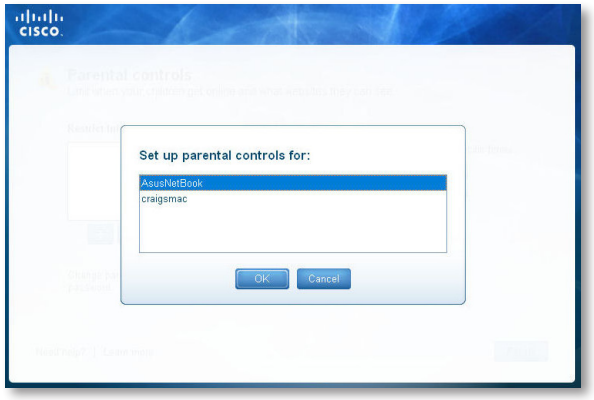
1. In the Parental controls main screen, click **Change parental controls password**, then follow the on-screen instructions.

How to select the computers to have parental controls

It's not necessary to set parental controls over each computer on your home network. You can set the controls on only those computers that children can access.

To select computers that will have parental controls:

1. In the *Parental controls* main screen, click **+** (add) under the *Restrict Internet access on* box.



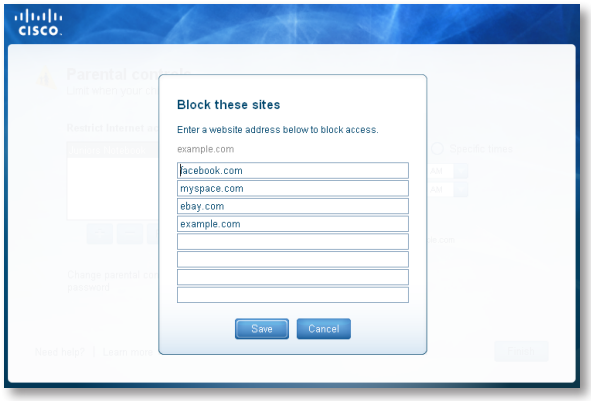
2. Click the computer name, then click **OK**. The computer is added to the list of computers with parental controls.
3. To remove parental controls from a computer, click the computer name in the *Restrict Internet access on* box, then click **–** (remove).

How to set parental controls

1. In the *Parental controls* main screen, click the computer name to set parental controls for.
2. Under *Block Internet access*, specify when the computer's Internet access will be blocked:

- **Never** does not block Internet access.
- **Always** blocks Internet access at all times.
- **Specific times** blocks Internet access only during specific times. If you select this option, set the schedule for **School nights** (Monday through Friday) and **Weekends** (Saturday and Sunday).

3. To create or change a list of specific websites to block, click **Edit** next to *Block specific sites*. The *Block these sites* screen opens.



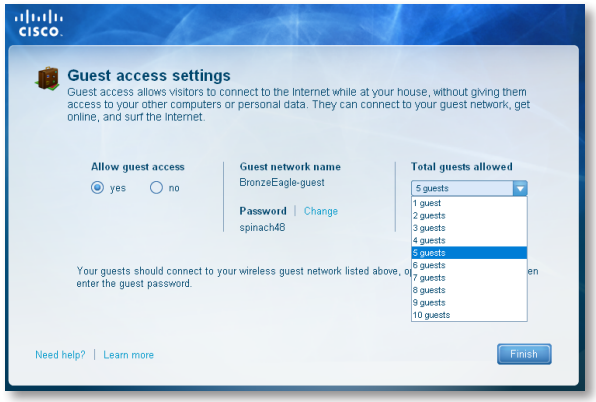
   a. On a blank line, enter a website address that you want to block.
   b. Click **Save** to save the list and return to the *Parental controls* main screen.
4. To save your changes, click **Finish**.
5. Repeat the above steps for each computer that you want to set parental controls for.

How to set up guest access to your network

You can use your router's guest access feature to provide your guests with access to the Internet, while restricting their access to other resources on your local network. The guest network is shown as an open, unsecure wireless network that your guests can easily connect to. To prevent unauthorized users from using your Internet access, your guest network requires that a password be entered for Internet access. The guest network is enabled by default.

To set up guest access to your network:

1. Run Cisco Connect, then click **Change** under *Guest Access*. The *Guest Access* screen opens.



2. Under *Allow guest access*, click **yes (default)** to allow guest Internet access. Otherwise, click **no** to disable guest access.
3. Take note of the Guest account's network name and password. You will need to provide this information to your guests.

TIPS

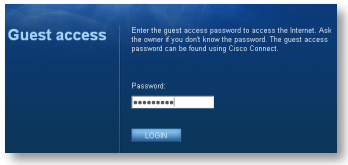
To keep your guest network secure, click **Change** to change the guest password when the guest no longer needs access to the account.

You can view the Guest account's name and password in Cisco Connect's main screen.

4. In the **Total guests** allowed drop-down box, select the number of simultaneous guest network users you want to allow.
5. Click **Finish** to apply your changes.

TIP

The first time your guest tries to access the Internet through a web browser, they will see the *Guest access* screen. To continue, they must enter the password you provided in the **Password** field, then click **LOGIN**.



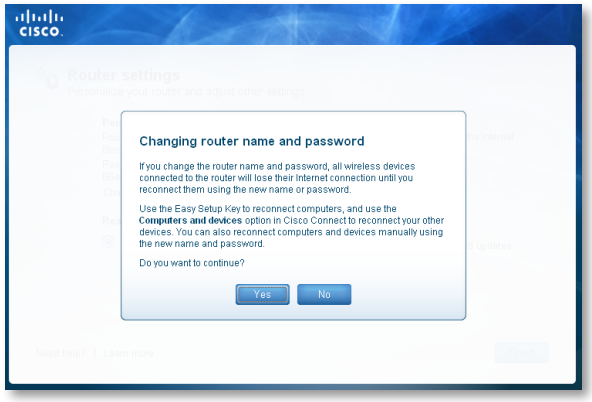
How to change your router's name and password

You can change the name and password of your router, but if you do so, all wireless devices connected to your router will lose their Internet connection until you reconnect them using the new router name and password.

CAUTION
If you change your router's name and password using the browser-based utility, you may not be able to manage your router using Cisco Connect. We recommend using the procedure below to change your router's login information.

To change your router's name and password:

1. Run Cisco Connect, then click **Change** under *Router settings*.
2. Under *Personalize*, click **Change**. A *Changing router name and password* warning appears



3. Click **Yes** if you want to continue.
4. Enter the new router name and password, then click **Change**.

TIP
After you make changes, update your Easy Setup Key to make it easier to reconnect all of the other computers on the network.

Setting Up: Advanced

How to open the browser-based utility

To access some advanced settings, you need to open the browser-based utility.

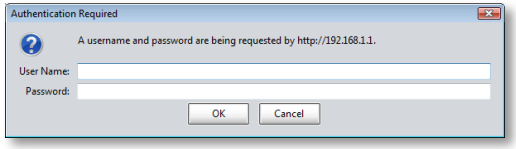
To open the browser-based utility:

1. Run Cisco Connect, click **Change** under *Router settings*, click **Advanced settings**, then click **OK**.

   – or –

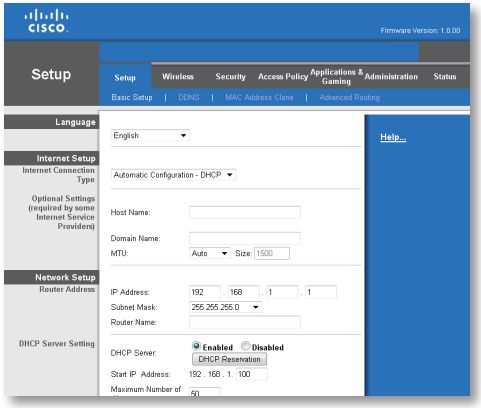
   Open a web browser on a computer connected to your network, then go to **192.168.1.1**.

   The router prompts you for a user name and password.



2. Enter the user name and password, then click **OK**. The utility's main menu opens.

   TIP
   If you set up your router without using Cisco Connect, your router's default password is **admin**. (You can leave the user name blank.)



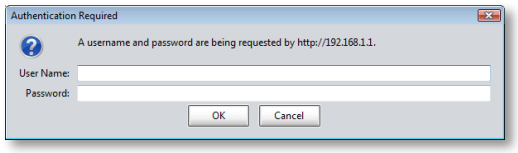
How to manually set up your router

Although running Cisco Connect is the easiest way to set up and maintain your router, advanced users may want to manually configure their router. Be careful when changing settings using this method.

To manually set up your router:

1. If you have started the Cisco Connect setup, exit Cisco Connect.
2. Connect your router's power adapter to a power outlet.
3. Connect an Ethernet cable to the computer and to an available numbered **Ethernet** (blue) port on the back of your router.

4. Open a web browser on the computer and open the address **192.168.1.1**. A login window appears.



5. Enter the default password (**admin**). (You can leave the user name blank.) The browser-based utility opens to the main menu.
6. After you finish changing settings, click **Save Settings** at the bottom of the screen.
7. To exit the browser-based utility, close the web browser window.

TIP
For field descriptions, click **Help** in the right side of the screen.

How to manually set up your Internet connection

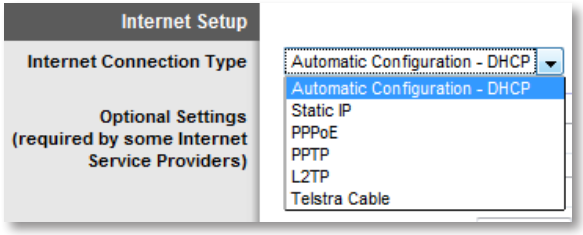
In most cases, Cisco Connect automatically sets up your Internet connection (see "How to start Cisco Connect" on page 4). For some *ISPs* (Internet Service Providers), especially those outside of the United States, you may need to manually configure your router's Internet connection. Your router supports six types of Internet connections.

To manually configure your router's Internet connection:

Setup > Basic Setup

1. Log into the browser-based utility (see "How to open the browser-based utility" on page 14).
2. Click the **Setup** tab, then click the **Basic Setup** page.
3. In the **Internet Connection Type** drop-down list, click the type of Internet connection provided by your ISP.

TIP
For field descriptions, click **Help** on the right side of the screen.



4. Complete the fields required by your ISP.
5. Complete the *Optional Settings* only if required by your ISP.
6. Click **Save Settings** at the bottom of the page.

How to set up the DHCP server on your router

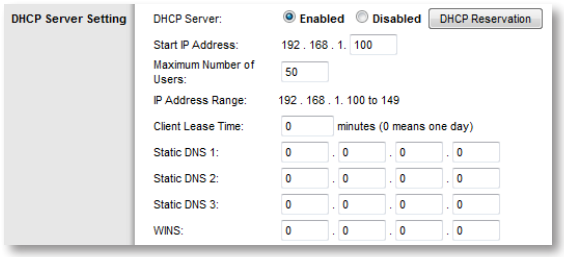
Your router can be used as a *DHCP* (Dynamic Host Configuration Protocol) server to automatically assign an IP address to each computer or device on your network. The DHCP server is enabled by default. If you already have a DHCP server on your network, or if you do not want to use your router as a DHCP server, you should disable this setting.

To configure your router's DHCP server settings:

Setup > Basic Setup > DHCP Server Settings

1. Log into the browser-based utility (see "How to open the browser-based utility" on page 14).
2. Click the **Setup** tab, then click the **Basic Setup** page.

3. Review the *DHCP Server Setting* fields (in the middle of the screen). You can:
   - Enable or disable the DHCP server.
   - Change the starting address for the DHCP server.
   - Change the number of users (253 maximum).
4. If you change any of the settings, click **Save Settings** at the bottom of the page.



TIP
For field descriptions, click **Help** on the right side of the screen.

How to set up DHCP reservation

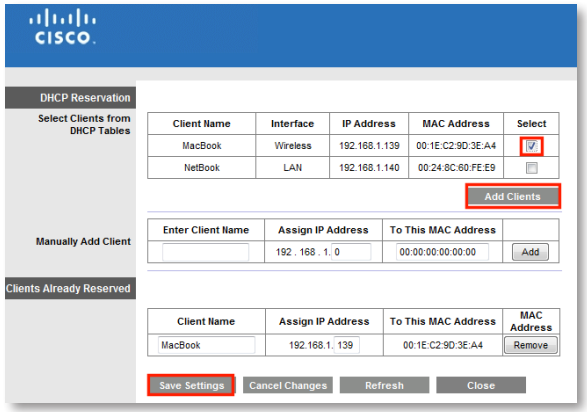
Why would I use it? *DHCP reservation* allows you to assign a unique, fixed IP address to a specific device on your network. Assigning a fixed IP address is a good way to manage devices such as print servers, web cameras, network printers, and game consoles. A fixed IP address is also recommended if you want to use port forwarding for devices that need to receive inbound traffic from the Internet ("How to set up port forwarding" on page 39).

To configure DHCP reservation:

Setup > Basic Setup > DHCP Reservation

1. Log into the browser-based utility (see "How to open the browser-based utility" on page 14).
2. Click the **Setup** tab, then click the **Basic Setup** page.
3. Click **DHCP Reservation** (in the middle of the screen).
4. Click **Select** next to the client you want to create a DHCP reservation for.
5. Click **Add Clients**. The client you selected is added to the *Clients Already Reserved* table.

   You can also manually enter a client name, IP address, and MAC address of a device to create a DHCP reservation.
6. Click **Save Settings**.



TIP
For field descriptions, click **Help** on the right side of the screen.

How to find your network on the Internet

Why would I need to find my network on the Internet? If you want to remotely access a USB drive attached to your router or view a web camera, you need to find your network on the Internet.

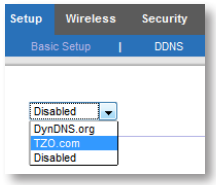
Working with several DDNS service providers, your router's DDNS feature lets you configure a domain name for your network, which you can then use to easily find your network on the Internet. If your ISP changes your network's IP address, the DDNS service providers detect the address change and continue to route your domain name to that address.

TIP
Before you configure DDNS on your router, you must sign up for DDNS service from a DDNS service provider that's supported by your router.

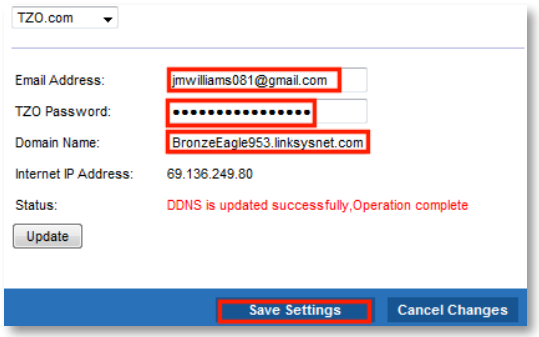
To set up DDNS:

Setup > DDNS

1. Sign up for DDNS service at either **www.dyndns.org** or **www.tzo.com**.
2. Log into the browser-based utility (see "How to open the browser-based utility" on page 14).
3. Click the **Setup** tab, then click the **DDNS** page.
4. In the **DDNS Service** drop-down list, click your DDNS service provider. The examples below are based on TZO.com. The settings used by DynDNS.org are slightly different.



5. Complete the fields with information provided by your DDNS provider, then click **Save Settings**. The *Status* field tells you what actions have been taken.



In this example, the domain name registered with TZO.com is *BronzeEagle953.linksysnet.com*. If an Internet camera had been configured (see "How to set up port forwarding for a single port" on page 39), you could access the camera by typing the domain name into the address bar of your web browser followed by the port number used for the device. For example, if the camera in the above example used port 1024, the URL would be:

BronzeEagle953.linksysnet.com:1024

How to clone a MAC address

On any home network, each network device has a unique *MAC* (Media Access Control) address. Some ISPs register the MAC address of the device (usually a router or a computer) connected directly to the modem. If your computer's MAC address is registered with your ISP and you do not want to re-register the MAC address, then you can *clone* the address (assign the registered MAC address of your previous device to your new router). If you want to use the MAC address from an old router that you are replacing with your new router, you should first determine the MAC address of your old router, then manually enter it into your new router.

NOTE

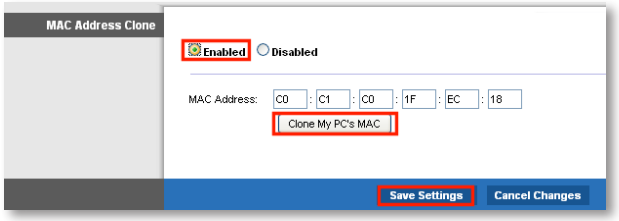
For many ISPs that provide dynamic IP addresses automatically, the stored MAC address in the modem is reset each time you reset the modem. If you are installing this router for the first time, reset your modem before connecting the router to your modem. To reset your modem, disconnect power for about one minute, then reconnect power.

To clone a MAC address from your computer:

Setup > MAC Address Clone

1. Log into the browser-based utility (see "How to open the browser-based utility" on page 14).
2. Click the **Setup** tab, then click the **MAC Address Clone** page.
3. Click **Enabled**.
4. Click either **Clone My PC's MAC** or enter the 12-digit MAC address of your old router.

5. Click **Save Settings**.



How to connect to your corporate office using a VPN

What is a VPN, and do I need to change my router settings? A *VPN* (Virtual Private Network) is a network that uses a public network, such as the Internet, to provide secure communications between a remote computer and another network. Corporations often provide VPN access to their networks to enable employees to work from remote offices or while traveling. Most corporate VPNs use the Internet to provide connectivity between remote employees and the corporate network.

For a typical VPN, the corporation installs a VPN gateway on their corporate network. Employees authorized to work remotely connect to the VPN gateway through the Internet using VPN software and security methods provided by their employers. Robust security and authentication schemes ensure a secure connection and access by only authorized users.

The default VPN settings in your router have been configured to pass through (allow) the most common types of VPN protocols, so usually no changes are needed.

To change your VPN passthrough settings:

Security > VPN Passthrough

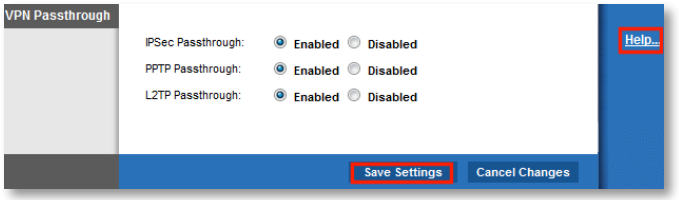
1. Log into the browser-based utility (see "How to open the browser-based utility" on page 14).
2. Click the **Security** tab, then click the **VPN Passthrough** page.
3. Select each setting that you want to change.

TIP

For brief descriptions of the VPN passthrough field settings, click **Help** in the right side of the screen. More complete descriptions are provided below.

- **IPSec Passthrough** – *IPSec* (Internet Protocol Security) is a suite of protocols used to implement secure exchange of packets at the IP layer. The VPN clients on the local network can establish an IPSec VPN tunnel through the router. This option is enabled by default.
- **PPTP Passthrough** – *PPTP* (Point-to-Point Tunneling Protocol) allows the *PPP* (Point-to-Point Protocol) to be tunneled through an IP network. The VPN clients on the local network can establish a PPTP VPN tunnel through the router. This option is enabled by default.
- **L2TP Passthrough** – *L2TP* (Layer 2 Tunneling Protocol) enables point-to-point sessions using the Internet on the Layer 2 level. The VPN clients on the local network can establish an L2TP VPN tunnel through the router. This option is enabled by default.

4. Click **Save Settings** to save your changes.



How to optimize your router for gaming and voice

How does my router prioritize traffic to the Internet? Your router has *QoS* (Quality of Service) settings that can prioritize traffic from your network out to the Internet. Performance for demanding, real-time applications, such as online gaming, VoIP calls, video streaming, and videoconferencing, can be improved by configuring Internet access priorities.

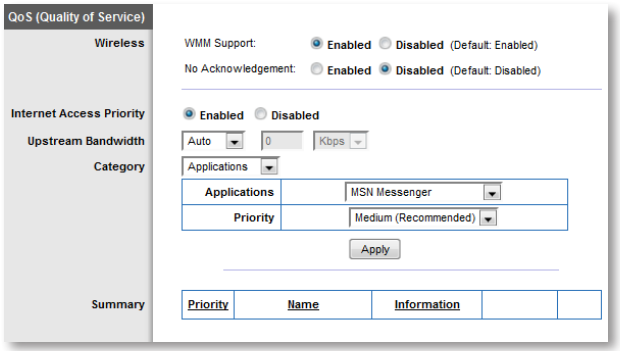
QoS is applied only to traffic that is uploaded to the Internet. The router cannot control the quality of the traffic after it reaches the Internet.

TIP
For more information on optimizing your router for online gaming, see "Port Forwarding and Port Triggering" on page 39.

To configure QOS:

Applications & Gaming > QoS

1. Log into the browser-based utility (see "How to open the browser-based utility" on page 14).
2. Click the **Applications & Gaming** tab, then click the **QoS** page.



TIP
For field descriptions, click **Help** on the right side of the screen.

3. To help manage traffic priority with devices that support WMM, select **Enabled** under *WMM Support*. Otherwise, select **Disabled**.

TIP
WMM (Wi-Fi MultiMedia) Support is a wireless QoS feature based on the IEEE 802.11e standard. WMM improves quality for audio, video, and voice applications by prioritizing wireless traffic. This feature requires that the wireless client devices in your network also support WMM.

4. To have the router re-send data if an error occurs, select **Disabled** under *No Acknowledgement*. Otherwise, select **Enabled**.
5. To set access priorities for a specific device or application, select **Enabled** next to *Internet Access Priority*.
6. In the **Category** drop-down list, select the type of item you want to set a priority for. A list of installed items fitting that description appears.

TIP
Do not set all priorities to **High**, because all items will have the same priority, and it would be easier to disable Internet Access Priority for the same result.

- **Applications** and **Online Games**—Let you assign a priority for an application or online game.
  a) Select the application or online game that you want to add from the drop-down list, then select the priority.
  b) Click **Apply**, then click **Save Settings**.

TIP
If you want to add a new application or game, you need to know its port and protocol information (see the application or game's documentation for help).

- **MAC Address** and **Voice Device**—Let you prioritize network traffic based on the device that is accessing the network. For example, if you want your gaming console to have higher priority than your computer for accessing the Internet, you can assign a higher priority to your game console using its MAC address. We recommend giving any voice devices a high priority.

  a) Select **MAC Address** or **Voice Device** from the drop-down list, then enter the name of the device you want to add.

  b) Enter the device's 12-digit MAC address, then select the priority.

  c) Click **Apply**, then click **Save Settings**.

TIP
You can often find a device's 12-digit MAC address on the bottom of the device. Or, if the device is connected to your network and turned on, you can click the **Administration** tab in the router's browser-based utility, click the **Local Network** page, then click **DHCP Client Table**.

7. Configure **Upstream Bandwidth**.
   - To allow the router to detect the maximum, select **Auto** (default). Auto sets speeds in multiples of 512 Kbps.
   - To specify the maximum, select **Manual**, then select the bandwidth you want it to use.

CAUTION
If you specify a maximum bandwidth that is too high, the router cannot apply priorities correctly, and QoS problems may result.

8. When you are done setting priorities, click **Save Settings**.

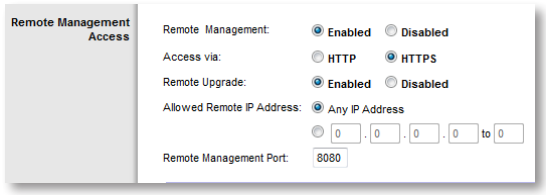
How to remotely change your router settings

Why would I want to remotely change my router settings? There may be times when you want to change parental control settings, or change settings for remote file access, while you are away from home.

To set up remote access:

Administration > Management

1. Log into the browser-based utility (see "How to open the browser-based utility" on page 14).
2. Click the **Administration** tab, then click the **Management** page and locate the *Remote Management Access* settings in the middle of the screen.
3. For *Remote Management*, select **Enabled**.
4. For *Access via*, select **HTTP** (default) or select **HTTPS** to use *SSL* (Secure Socket Layer) to encrypt data transmitted for higher security.
5. To be able to upgrade your router's firmware remotely, select **Enabled** next to *Remote Upgrade*.
6. To allow remote access from anywhere on the Internet, select **Any IP Address** (default) next to *Allowed Remote IP Address*. Otherwise, enter a range of allowed IP addresses.
7. For *Remote Management Port*, keep the setting of **8080** (default) unless you already have a device on your network that uses port 8080 (such as a web camera).
8. Click **Save Settings** at the bottom of the screen to accept your changes.



9. Click the **Administration** tab, then click the **Management** page and take note of the *Internet IP Address* and the *Remote Management Port* settings. You will use this information to access your router remotely.

To access your router remotely:

1. Open a web browser and enter the Internet address of your router, then press **Enter**.
   - If you selected **HTTP** for your *Access via* setting, enter **http://** then the IP address.

   – OR –

   - If you selected **HTTPS** for your *Access via* setting above, enter **https://** then the IP address.
2. Add a colon (:), then the *Remote Management Port* number. Example:

   https://69.192.16.170:8080

   TIP
   If you enabled the Dynamic Domain Name Service (see "How to find your network on the Internet" on page 16), you could type in your domain name in place of your router's Internet IP address. For example:
   https://BronzeEagle953.linksysnet.com:8080

   You are prompted for a user name and the password. Use the same login information that you use to access your router at home.

   After you have logged into your router's browser-based utility remotely, you can change any router setting, just as you would normally from your local network.

How to enable Voice over IP on your network

Do I need to configure Voice over IP? *VoIP* (Voice over Internet Protocol) is a technology for using the Internet as an interface for telephone communications. To use VoIP, you need to get an account with a VoIP service provider. The VoIP service provider typically provides you with a telephone adapter (TA) that connects to your network. If you do not use your network to make phone calls, you don't need to change the default settings.

The *SIP* (Session Initiation Protocol) *ALG* (Application Layer Gateway) feature allows SIP packets, used by some VOIP service providers, to traverse (go through) your router's firewall.

To configure the router for VoIP:

Administration > Management

1. Log into the browser-based utility (see "How to open the browser-based utility" on page 14).
2. Click the **Administration** tab, then click the **Management** page.
3. If your VoIP service uses SIP, select **Enabled** next to *SIP ALG*.

   – OR –

   If your VoIP service uses other NAT traversal solutions such as *STUN* (Session Traversal Utilities for NAT), *TURN* (Traversal Using Relay NAT), or *ICE* (Interactive Connectivity Establishment), select **Disabled** (default).

NOTE
You may need to contact your VoIP service provider to determine the type of NAT traversal configuration they use.

How to configure UPnP

What is UPnP? *UPnP* (Universal Plug and Play) allows devices connected to a network to discover each other and automatically create working configurations. Examples of UPnP-capable devices include web cameras, online gaming applications, and VoIP devices. UPnP is enabled by default.

To configure UPnP:

Administration > Management

1. Log into the browser-based utility (see "How to open the browser-based utility" on page 14).
2. Click the **Administration** tab, then click the **Management** page.
3. To use UPnP, select **Enabled** (default) next to *UPnP*. Otherwise, select **Disabled**.
4. To allow changing router settings while using UPnP, select **Enabled** (default) next to *Allow Users to Configure*. Otherwise, select **Disabled**.

5. To prevent local network users from disabling your Internet connection through UPnP, select **Disabled** (default) next to *Allow Users to Disable Internet Access*. Otherwise, select **Enabled**.

How to use a router as an access point

How can I use my old router as an access point? If you have a large area to cover with your wireless signal, or if part of your home has weak signals due to interference, you can use your old router to extend the range of your wireless network. This is a complex process, so this procedure assumes that you have some networking knowledge.

> **TIP**
> Check the documentation for your old router. Some brands of routers include either a switch on the outside of the case or a software option to convert it to an access point. If either of these options is available, follow your old router's instructions to convert it to an access point.

You need to take note of your new router's settings, then apply some of those settings to the old router so it can work as an access point.

To view your new router's settings:

Wireless > Basic Wireless Settings
Wireless > Wireless Security
Status > Wireless Network
Setup > Basic Setup

1. Make sure that your new router is connected to the Internet.
2. In the browser-based utility, click the **Wireless** tab, then click the **Basic Wireless Settings** page and take note of the *Network Name (SSID)*.
3. Click the **Wireless** tab, then click the **Wireless Security** page and take note of the *Security Mode* and the passphrase.
4. Click the **Status** tab, then click the **Wireless Network** page and take note of the *Channel*.
5. Click the **Setup** tab, then click the **Basic Setup** page and take note of the DHCP server's IP Address range (192.168.1.100 to 192.168.1.149 by default)

To use your old router as an access point:

1. With your computer connected to your old router, log into its browser-based administration utility.

   > **NOTE**
   > Save your changes after finishing each step below.

2. Open the setup page for the local network (LAN).
3. In the **Router IP address** field, enter an unused IP address for the LAN network of your new router.

   For example, if your new router has an IP address of 192.168.1.1, you should choose an IP address on the 192.168.1.0 network. You can choose any address within the range of 192.168.1.2 to 192.168.1.254. You should exclude addresses in the range that will be used by the DHCP Server of your new router (192.168.1.100 to 192.168.1.149). A safe choice might be 192.168.1.250. Take note of this address, because this will be the address that you will use to manage your old router in the future.
4. In the **Subnet Mask** field, enter **255.255.255.0** or, if available, select that subnet mask from a drop-down list.
5. Disable the DHCP server on your old router. (Because your old router will be operating as an access point instead of a router, you don't want it to distribute IP addresses. There should be only one active DHCP server on your network, and that should be your new router.)
6. To reconfigure the wireless network on your old router:
   a. Open the wireless network setup page.
   b. Change the network name (SSID) to match the name of your new network. Having the same network name and security settings enables you to seamlessly roam between your new router and your old router.
   c. Change the security mode to match the security mode on your new router.
   d. Change the passphrase (sometimes called the pre-shared key) on your old router to match the passphrase on your new router.

e. Change the wireless channel to a non-conflicting channel. Some manufacturers have an "Auto" function for channel selection that automatically selects a wireless channel that does not interfere with other nearby wireless networks. If your old router supports an Auto function, select that. Otherwise, you may need to manually select the wireless operating channel on your old router. In the 2.4 GHz wireless spectrum, there are only three non-overlapping channels: 1, 6, and 11. Pick a channel that does not overlap the operating channel of your new router. For example, if your new router is operating on channel 11, configure your old router for either channel 1 or channel 6.

7. Connect an Ethernet network cable to one of the LAN/Ethernet ports on your old router and an Ethernet port on your new router.

CAUTION
Do **not** connect the cable to the Internet port on your old router. If you do, you may not be able to set up the router as an access point on the current network.

How to put your new router behind an existing router

Why would I put my new router behind an existing router? There are several possible scenarios in which you might want to use your new router "behind" another router:

1. You might be in an environment that shares the landlord's Internet connection with all tenants. In this case, you should put your own router behind the landlord's router in order to create your own private network and to isolate computers on your network from the rest of the building.
2. You are sharing an office building Internet connection, and you want to control Internet access or the content viewed by your employees.
3. You already have an existing network and you want to extend the network's range or add wireless capabilities to your network.
4. You want to separate older, less secure network devices from the rest of the network.

To add your router to an existing router or gateway

In most cases, you can easily add your router to an existing wireless network by running Cisco Connect. If you are unable to set up the additional router using the instructions below, see "To share an Internet connection" on page 23 or "To extend your network" on page 25.

To add a router to your existing wireless network:

1. Insert the Cisco Connect setup CD into a CD/DVD drive on your computer, then follow the on-screen instructions.
2. When you are told to connect your router's **Internet** port to the **LAN/Ethernet** port on your modem, connect your router's **Internet** port to the **LAN/Ethernet** port on your existing (upstream) router or gateway.
3. Follow the on-screen instructions until setup is complete.

To share an Internet connection

NOTE
This is a complex process, so this procedure assumes that you have some networking knowledge.

To add another router to share an Internet connection:

This topic covers cases one and two above

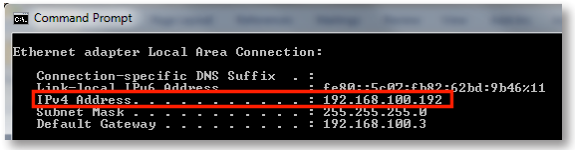
1. Determine the IP address range for your upstream (office or building) network.

   To determine the address range by using a Windows computer:

   a. Connect your computer into your upstream network's router.

   b. Click **Start**, **Run**, type **CMD**, then click **OK**. The command prompt window appears.

   c. Type **ipconfig**, then press **Enter**.



TIP
Although you can determine your computer's IP address in many ways, this method is very fast.

d. Take note of the IP address. In this example, the IP address is 192.168.100.192.

To determine the address range by using a Mac computer:

a. Connect your computer into your upstream network's router.

b. From the *Dock*, click **System preferences**, click **Network**, then click **Ethernet** in the window to the left. A network status window appears.

c. Take note of the IP address. In this example, the IP address is 192.168.100.139.

Example: The above examples show that upstream IP addresses are on the 192.168.100.0 network. (The "0" indicates the entire network.) Your upstream network's address may be different. The default address of your new Linksys router is 192.168.1.1. In setting up one router behind another, you must make sure that the local network on your new router is different than the network of your upstream router. In the above example, because the default local network on your Linksys router 192.168.1.0 is on a different subnet than the office network's 192.168.100.0, you will be able to place your Linksys router behind the other router.

2. Connect an Ethernet network cable to a LAN/Ethernet port on your upstream network to the yellow **Internet** port on your router.

CAUTION
Connect the upstream network to your router's yellow **Internet** port, *not* one of the blue Ethernet ports. If you connect to an Ethernet port, you create IP addressing problems for the office network.

TIPS
An office network often has a wall plate with an Ethernet port that you can connect to.

If you are doing this in a home environment (without wall ports), connect an Ethernet network cable between a LAN port on your upstream router and the **Internet** port on your Linksys router.

3. Run Cisco Connect on each computer that you want to connect to the Linksys router. Each computer needs either a wired or wireless connection to the Linksys router. For more information, see "How to connect a computer to your network" on page 6.

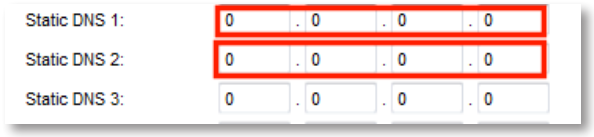
The computers that are connected to the Linksys router are now on the same network, and are isolated from the upstream network. However, you will still have access to the Internet through the upstream router (by way of your Linksys router). Because two routers are between your computer and the Internet, Internet traffic undergoes two network address translations. This is sometimes referred to as *Double NAT*.

Your computers can also use the built-in capabilities of your Linksys router, such as parental controls. If you need further control over the type of content your employees or family access, you can create an account with an Internet filtering site such as **www.opendns.com** or **www.bsecure.com**. After you create an account with them, use their DNS in place of your ISP's DNS.

To use their DNS:

Setup > Basic Setup

1. Log into the browser-based utility (see "How to open the browser-based utility" on page 14).
2. Click the **Setup** tab, then click the **Basic Setup** page.
3. Complete the **Static DNS** fields with the information provided by your content filtering provider.



4. Click **Save Settings**.

To extend your network

This topic covers cases three and four above.

NOTE
This is a complex process, so this procedure assumes that you have some networking knowledge.

To extend your network or add wireless capabilities:

1. If you want to extend your network, you may also follow the instructions above. One example of this might be to provide a separate wireless network for your children to keep their wireless network traffic separate from your wireless network. You might also want to isolate one network from another network so that network shares aren't visible across networks. In this case, use an Ethernet cable to connect the **Internet** port of the downstream router to one of the LAN ports of the upstream router. Make sure that the local network subnets on the two routers are different.

   - OR -

   You can extend your network by turning the downstream router into an access point. (See "How to use a router as an access point" on page 22). When you use a router as an access point, computers connected to the access point are on the same IP subnet as all other devices connected to the router. File, printer, and media sharing is much easier if all devices are on the same subnet.

How to expose a device to the Internet

Why would I expose a device to the Internet? If you are operating a web server, a mail server, or a web camera, you may want to expose that device to the Internet so anybody can access it. Your router includes a *DMZ* (Demilitarized Zone) feature that forwards all inbound ports presented on the WAN interface, except those that are specifically forwarded, to an individual IP address or MAC address. This feature is normally not used, because it presents significant security risks to the device that you designate for the DMZ. The DMZ device is not protected by the built-in firewalls, Internet filters, or router web filters, and is open to attacks from hackers.

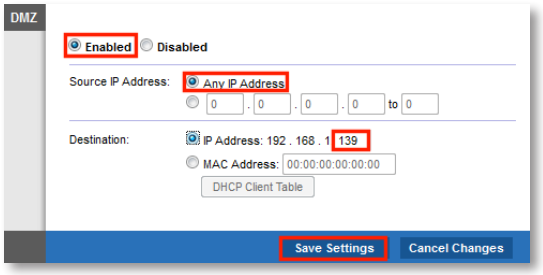
A much better way of "exposing" devices to the Internet would be to use port forwarding. See "How to set up port forwarding" on page 39.

To set up a device in the DMZ:

Applications & Gaming > DMZ

1. Configure your device with a static IP address. See your device's documentation for help with setting a static IP address or use DHCP reservation (see "How to set up the DHCP server on your router" on page 15).
2. Log into the browser-based utility (see "How to open the browser-based utility" on page 14).
3. Click the **Applications & Gaming** tab, then click the **DMZ** page.
4. Select **Enabled**.
5. In the *Source IP Address* section, select **Any IP Address** to allow access to your DMZ device from the entire Internet, or select the **source range** button and enter a range of allowed source addresses.
6. In the *Destination* section, enter the last three digits of the IP address of the device that will be in the DMZ. The rest of the IP address is already completed.

7. Click **Save Settings** to apply your changes.



If you prefer to specify the 12-digit MAC address of the device you want to place in the DMZ instead of setting up a DHCP address reservation, you can replace Step 6 with the following steps:

a. Click **Enabled**.

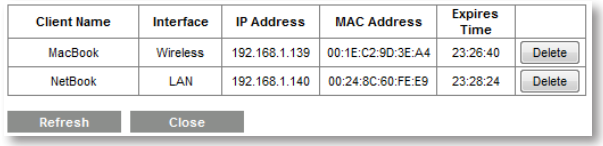
b. In the *Source IP Address* section, select **Any IP Address** (default) to allow access to your DMZ device from the entire Internet, or select the **source range** button and enter a range of allowed source addresses.

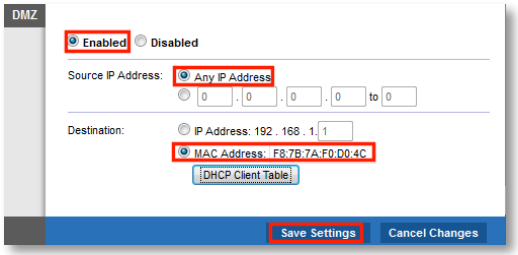
c. In the *Destination* section, select **MAC Address**, then click **DHCP Client Table**. A separate window opens showing the current DHCP client list.

d. Click **Select** next to the device that you want to place in the DMZ. In this example, the first device was selected. The corresponding MAC address was copied into the *MAC Address* field as shown below.

e. Click **Save Settings** to apply your changes.

TIP
The DHCP Client Table is only available if you select **MAC Address**.





Improving Security

How do I know if my network is secure?

If you configured your router using Cisco Connect, your network is secure. During setup, Cisco Connect creates a name for your network, enables industry-standard WPA/WPA2 wireless security, and assigns a highly secure password for your wireless network and the administrator's account.

To confirm that your network is secure:

1. Run Cisco Connect.

2. In the upper-right corner of the screen, check for the green light that indicates your router is online and secure. If the green light is on, no additional action is required to secure your network.

Network security following a manual setup

If you configured your router manually (not recommended), you must manually configure security.

To manually set your router's password:

Administration > Management

1. Log into the browser-based utility (see "How to open the browser-based utility" on page 14).
2. Click the **Administration** tab, then click the **Management** page.
3. In the *Router Access* section, enter a secure password for your router, then re-enter the password to confirm it. Your password should be at least eight characters in length. The most secure type of password should include a mix of uppercase and lowercase letters, numbers, and punctuation.
4. Click **Save Settings** at the bottom of the screen.

To manually set your router's network name (SSID):

Wireless > Basic Wireless Settings

1. Log into the browser-based utility (see "How to open the browser-based utility" on page 14).
2. Click the **Wireless** tab, then click the **Basic Wireless Settings** page.
3. For *Configuration View*, select **Manual**.
4. Enter a new network name in the **Network Name (SSID)** field, then click **Save Settings** at the bottom of the screen.

To manually set your router's wireless security settings:

Wireless > Wireless Security

1. Log into the browser-based utility (see "How to open the browser-based utility" on page 14).
2. Click the **Wireless** tab, then click the **Wireless Security** page.
3. Select your preferred security type from the **Security Mode** drop-down list For most home networks, we recommend **WPA2/WPA Mixed Mode**.
4. Enter a passphrase (security key) for your wireless network in the **Passphrase** field. The most secure type of security key should include a mix of uppercase and lowercase letters, numbers, and punctuation.
5. Click **Save Settings** at the bottom of the screen.

How to set up wireless security using Wi-Fi Protected Setup

Why would I use Wi-Fi Protected Setup? Wi-Fi Protected Setup™ is a feature of your router that makes it easy to add devices to your wireless network. If you have network devices, such as wireless printers, that support Wi-Fi Protected Setup, then you can use Wi-Fi Protected Setup to add the devices.

Wi-Fi Protected Setup activity light

The power indicator light on the back of the router (or on top for the E4200) indicates the status of Wi-Fi Protected Setup while you are connecting devices.

- When Wi-Fi Protected Setup is connecting a network device, the light flashes slowly.
- If there is an error, the light flashes quickly for two minutes. Wait until it stops flashing, then try again.
- When Wi-Fi Protected Setup has finished connecting a device, the light is continuously lit .
- Wait until the light is continuously lit before starting the next Wi-Fi Protected Setup session.

Connect network devices using one of the three methods below.

NOTE
Wi-Fi Protected Setup configures one device at a time. Repeat the instructions for each device that supports Wi-Fi Protected Setup.

Connecting a device using the Wi-Fi Protected Setup button

Use this method if your device has a Wi-Fi Protected Setup button or prompts you to press the Wi-Fi Protected Setup button on your router.

To connect a device using the Wi-Fi Protected Setup button:

Wireless > Basic Wireless Settings

1. Press the **Wi-Fi Protected Setup** button on the network device you are connecting to.
2. Press the **Wi-Fi Protected Setup** button on the back of the router.

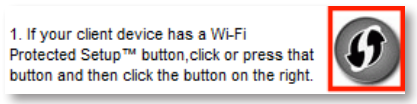
   - OR -

   a. Log into the browser-based utility (see "How to open the browser-based utility" on page 14).

   b. Click the **Wireless** tab, then click the **Basic Wireless Settings** page.

   c. Click **Wi-Fi Protected Setup**.

   d. Click the **Wi-Fi Protected Setup** button in the router's *Wi-Fi Protected Setup* screen.



   e. After the device has been configured, click **OK**.

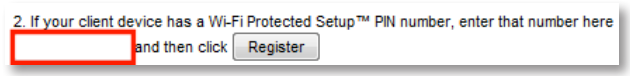
How to connect a device using its Wi-Fi Protected Setup PIN

Use this method if your device has a Wi-Fi Protected Setup *PIN* (Personal Identification Number).

To connect a device using the device's Wi-Fi Protected Setup PIN:

Wireless > Basic Wireless Settings

1. Log into the browser-based utility (see "How to open the browser-based utility" on page 14).
2. Click the **Wireless** tab, then click the **Basic Wireless Settings** page.
3. Click **Wi-Fi Protected Setup**.
4. Enter the PIN from the device into the **PIN** field on the router's *Wi-Fi Protected Setup* screen, then click **Register**.



5. After the device has been connected, click **OK**.

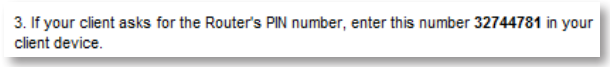
How to connect a device using the router's Wi-Fi Protected Setup PIN

Use this method if your client device asks for the router's PIN.

To connect a device using the device's Wi-Fi Protected Setup PIN:

Wireless > Basic Wireless Settings

1. Log into the browser-based utility (see "How to open the browser-based utility" on page 14).
2. Click the **Wireless** tab, then click the **Basic Wireless Settings** page.
3. Click **Wi-Fi Protected Setup**.
4. On the client device, enter the PIN listed on the router's *Wi-Fi Protected Setup* screen. It is also listed on the bottom of the router. In the example below, the router's PIN is 32744781.



5. Follow the device's instructions to complete setup.

How to connect a device manually

If you have devices that do not support Wi-Fi Protected Setup, note the wireless settings in the *Basic Wireless Settings* screen, then manually configure those devices.

For each wireless network, the Network Name (SSID), Security, and Passphrase are displayed at the bottom of the screen.

How to control access to your wireless network

Why would I need to control access to my wireless network? If you used Cisco Connect to configure your router, your wireless network is already secure. By default, Cisco Connect enables industry-standard *WPA* (Wi-Fi Protected Access) security using WPA2/WPA mixed mode. Cisco Connect configures your network with a complex, 10-character password that is almost impossible to compromise. If you set up your wireless network manually and have not enabled wireless security, your wireless network will be an "open" network that almost anyone nearby with a Wi-Fi-enabled device could access.

What is MAC filtering? The best way to secure your wireless network is to use Cisco Connect to automatically configure and secure it. However, if you choose not to use the built-in security features of your router, you can still control access to your wireless network using MAC filtering.

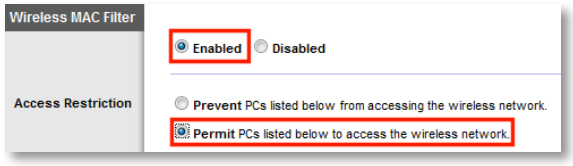
Every network device has a unique, 12-digit *MAC* (Media Access Control) address. Using MAC filtering, you can allow only known MAC addresses onto your network. You can also exclude specific MAC addresses or deny them access to your wireless network.

Example: Because each MAC filtering configuration is unique, the following procedure uses the simplified example of setting up MAC filtering to allow one wireless device access to the network.

To set up MAC filtering to allow one wireless device access to your network:

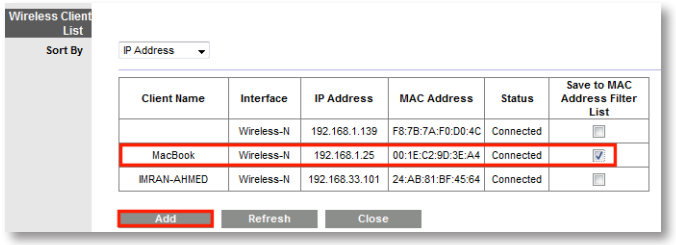
Wireless > Wireless MAC Filter

1. Log into the browser-based utility (see "How to open the browser-based utility" on page 14).
2. Click the **Wireless** tab, then click the **Wireless MAC Filter** page.
3. Click **Enabled**.
4. Select **Permit**.

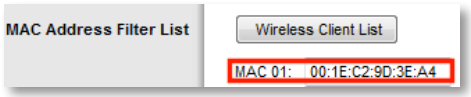


TIP
You can also use MAC filtering to prevent specific PCs from accessing your network by selecting **Prevent**. However, it's easier to permit only known devices than to exclude unknown devices.

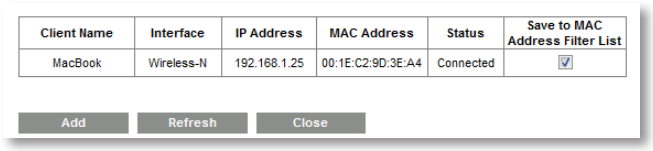
5. Click **Wireless Client List**. A separate window opens and displays the currently connected devices. In the example below, the only device permitted onto the network is the MacBook. However, two other devices are also connected to the network.



6. Next to the device entry, select **Save to MAC Address Filter List**, then click **Add**. The Mac Address Filter List is updated with the MAC address of the device you added.



7. Click **Save Settings** at the bottom of the page.
8. Click **Wireless Client List** again to check the updated device list. Only the device you selected remains on the network.



How to improve security using the built-in firewall

Why would I need to change my security settings? By default, the firewall settings in your router have been optimized for most home environments, so no changes are needed. The *SPI* (Stateful Packet Inspection) firewall is enabled by default. In addition, anonymous Internet requests and IDENT requests are filtered by default. All web filters are disabled, because enabling them may cause problems for sites that depend on ActiveX controls, Java, or cookies.

To change your firewall settings:

Security->Firewall

1. Log into the browser-based utility (see "How to open the browser-based utility" on page 14).
2. Click the **Security** tab, then click the **Firewall** page.
3. Select each setting that you want to change.

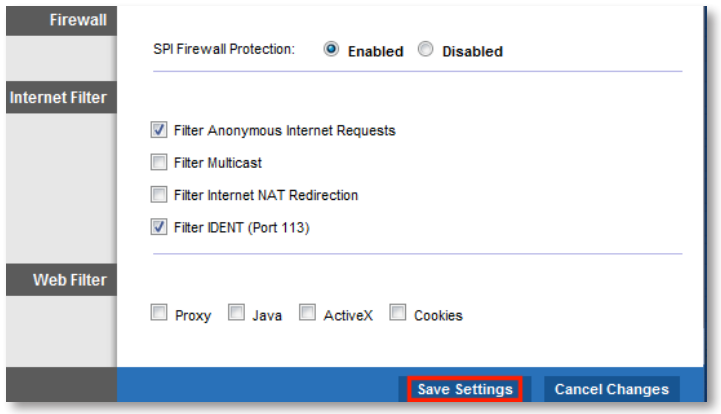
TIP
For descriptions of the filters, click **Help** on the right side of the screen. More complete descriptions are included below.

- **SPI Firewall Protection**—This helps protect your local network from Internet threats. This option is enabled by default.

CAUTION
To help protect your network, you should keep this option enabled.

- **Filter Anonymous Internet Requests**—This filter blocks Internet requests from unknown sources such as ping requests. This option is enabled by default.
- **Filter Multicast**—Multicasting allows a single transmission to simultaneously reach specific recipients within your local network. Select this option to block multicasting. This option is disabled by default.
- **Filter Internet NAT Redirection**—This filter prevents a local computer from using a URL or Internet IP address to access the local server. Select this option to enable the filter. This option is disabled by default.
- **Filter IDENT (Port 113)**—This filter prevents port 113 from being scanned by devices from the Internet. This option is enabled by default.
- **Proxy** - This filter blocks the use of Internet proxy servers. To deny proxy requests, select this option. Proxy access is allowed by default.
- **Java** - This filter blocks Java, so you may not be able to access Java content on websites. To deny Java requests, select this option. Java content is allowed by default.
- **ActiveX** - This filter blocks ActiveX, so you may not be able to access ActiveX content on websites. To deny ActiveX requests, select this option. ActiveX content is allowed by default.
- **Cookies** - This filter blocks cookies, which are data stored on your computer and used by websites when you interact with them. To deny cookie requests, select this option. Cookie usage is allowed by default.

4. Click **Save Settings** to update your changes.



Using an External Drive

How to configure storage

Why would I need to configure storage? By default, when you connect a storage device to your router, the entire contents of the device are available for read and write access to anyone on your local network (no login credentials are required). However, you can also create shared folders that you can configure to share only with specified groups.

To control access to the USB drive attached to your router, you need to perform two tasks:

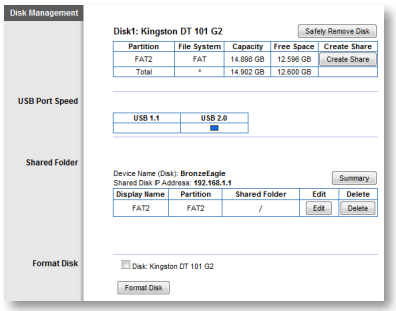
1. Create one or more shared folders (see "How to create shared folders" below)
2. Manage group and User Access to Shared Folders (see "How to share folders and set access rights" on page 37)

How to create shared folders

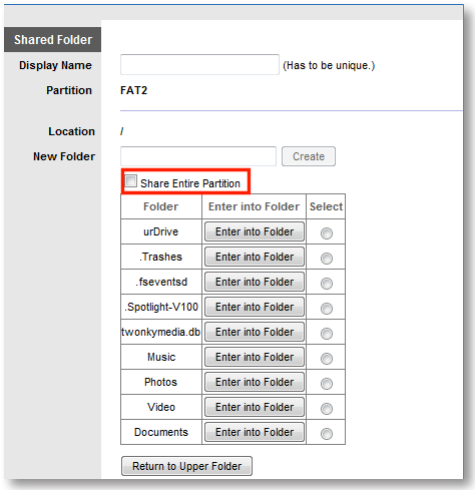
To create a shared folder:

Storage > Disk

1. Log into the browser-based utility (see "How to open the browser-based utility" on page 14).
2. Click the **Storage** tab, then click the **Disk** page.



3. Click **Create Share** next to the partition you want to share. The *Shared Folder* screen opens.
4. If you want to share the entire partition, select **Share Entire Partition**, then click **Save Settings** at the bottom of the screen.



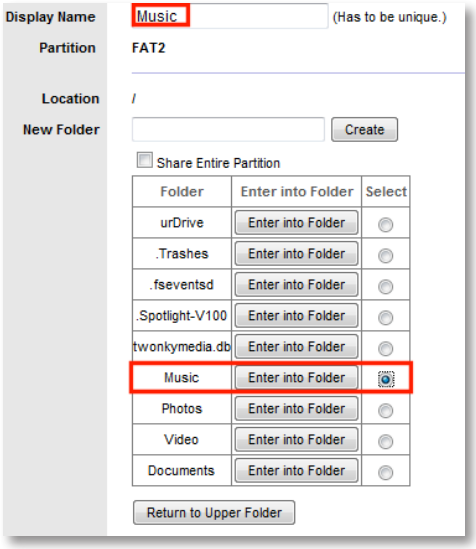
- OR –

If you want to share a specific folder:

a. Enter a unique name in the **Display Name** field.

b. Click **Select** next to the folder name you want to share.
   - To open a subfolder, click **Enter into Folder**.
   - To navigate to a previous folder, click **Return to Upper Folder**.
   - To create a new folder, type the name into the **New Folder** field, then click **Create**.

c. Click **Save Settings** at the bottom of the screen, then repeat the above steps to add more folders that you want to share.



How to manage group and user access to shared folders

To manage access to shared folders, you need to disable Anonymous Disk Access, then create groups and user accounts on your router. Access to the router is controlled by user accounts, but access to shared folders is controlled by groups.

1. Disable Anonymous Disk Access (see "How to disable anonymous disk access" on page 33).
2. Create a group that you will use to assign rights to a shared folder.
3. Create users and assign those users to the group.
4. Add the group to the shared folder that you want to control.

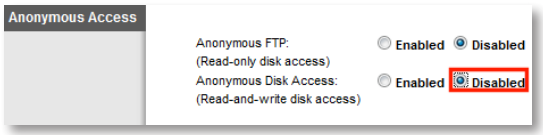
How to disable anonymous disk access

By default, no password is needed for read and write access to the drive. Before you can manage group and user access to shared folders, you must disable anonymous disk access.

To disable anonymous disk access:

Storage > Administration

1. Log into the browser-based utility (see "How to open the browser-based utility" on page 14).
2. Click the **Storage** tab, then click the **Administration** page.
3. Next to *Anonymous Disk Access*, select **Disabled**.



4. Click **Save Settings** at the bottom of the screen.

How to create a group

By default, the default Admin group has read and write access to all shared folders. By default, the Guest group has read only access and has no access rights to any of the shared folders.

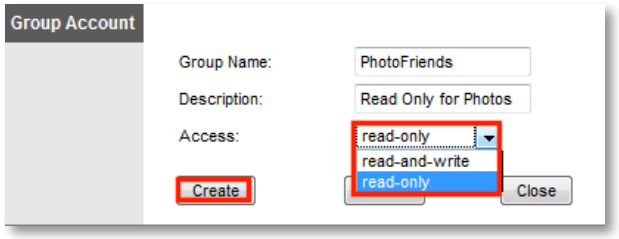
IMPORTANT
More than one group can be configured with access to a shared folder, but a user can be a member of only one group.

To create a group:

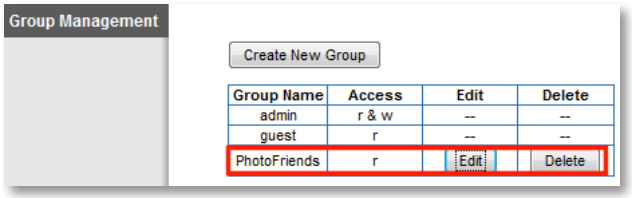
Storage > Administration

1. Log into the browser-based utility (see "How to open the browser-based utility" on page 14).
2. Click the **Storage** tab, then click the **Administration** page.

3. Under *Group Management*, click **Create New Group**.



4. Complete the **Group Name** and **Description** fields.
5. From the **Access** drop-down list, select **read-only** to grant read-only rights to the group, or select **read-and-write** to grant read and write rights to the group.
6. Click **Create**. The group is now created, and its access rights are displayed in the *Access* column.
7. To change a group's name or access rights, click **Edit** next to the group name.
8. To delete a group, click **Delete** next to the group name.



How to create a new user

Two user accounts (*Admin* and *Guest*) are preconfigured for router access. The password for the *Admin* user is the same password that you use to access the router. By default, the user *Admin* is a member of the group named *Admin*, and the user *Guest* is a member of the group named *Guest*. To keep it simple, consider creating user accounts on your router that use the same user names and passwords that are used by your computer's operating system.

NOTE
Users can be a member of only one group.

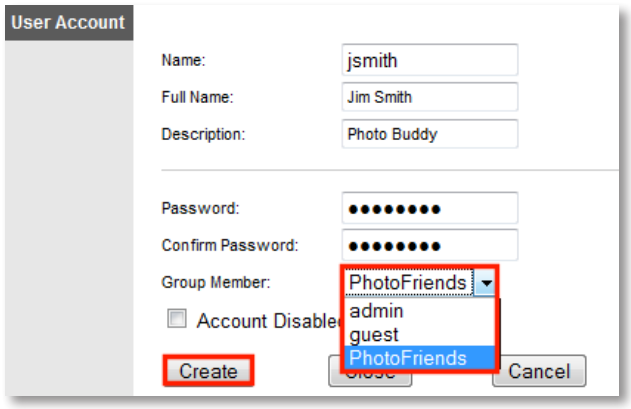
To create a new user:

Storage > Administration

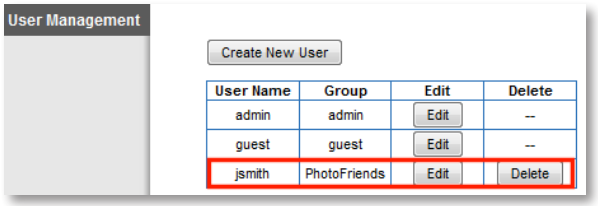
1. Log into the browser-based utility (see "How to open the browser-based utility" on page 14).
2. Click the **Storage** tab, then click the **Administration** page.
3. Under *User Management*, click **Create New User**.

4. Complete the **Name**, **Full Name**, and **Description** fields.
5. Enter and confirm a password.

6. From the **Group Member** drop-down list, select the group to assign the user to, then click **Create**. The new user is displayed in the user list.



7. To change the user name, description, or group membership, or to temporarily disable the account, click **Edit**.



8. To delete the user, click **Delete**.

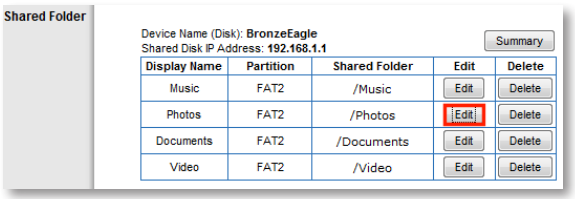
How to grant group access to a share

To grant group access to a share

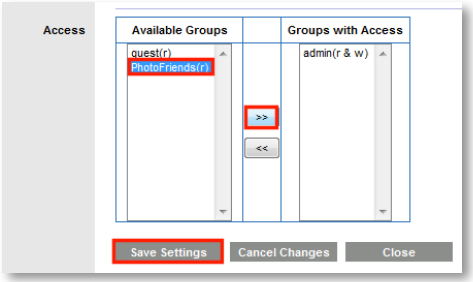
Storage > Disk

1. Log into the browser-based utility (see "How to open the browser-based utility" on page 14).
2. Make sure that *Anonymous Disk Access* has been disabled. (See "How to disable anonymous disk access" on page 33.)
3. Click the **Storage** tab, then click the **Disk** page.

4. In the *Shared Folder* section, click **Edit** next to the shared folder you want to change group access for.



5. To grant a group access the shared folder, click the group's name in the *Available Groups* column, then click **>>** to move the group to the *Groups with Access* column.
6. To remove a group's access to the shared folder, click the group's name in the *Groups with Access* column, then click **<<** to move the group to the *Available Groups* column.



7. Click **Save Settings** to apply your changes.

How to configure your router's storage for remote access

Why would I need to access my router's storage remotely? If your router's storage is set up for remote access, you can access your files anywhere you have an Internet connection. To do this, you must enable the router's built-in FTP (File Transfer Protocol) server. After your router is set up, you can access files from anywhere by using either a web browser or FTP software.

To set up your router for remote file access, you need to:

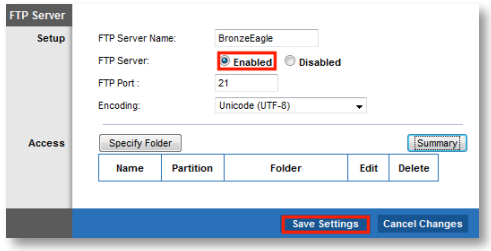
1. Configure the FTP server
2. Select folders (or the entire drive) to share and set access rights for those folders

How to configure the FTP server

To configure the FTP server:

Storage > FTP Server

1. Log into the browser-based utility (see "How to open the browser-based utility" on page 14).
2. Click the **Storage** tab, then click the **FTP Server** page.
3. Next to *FTP Server*, click **Enabled**.



TIP

If you used Cisco Connect to set up your router, the FTP Server Name field is already completed with the name of your wireless network. If you set up your router manually, the default name is Cisco followed by the last five digits of the router's serial number.

4. You can also:
   - Change the **FTP Port** (default is **21**) for the FTP server
   - Change the **Encoding** (character set) for the transfer of files in other languages. The router supports:
     - Unicode (UTF-8) (default)
     - Chinese Simplified (GB18030)
     - Vietnamese (CP1258)
     - ISO 8859_1.

TIP

For field descriptions, click **Help** on the right side of the screen.

5. To apply your changes, click **Save Settings**.

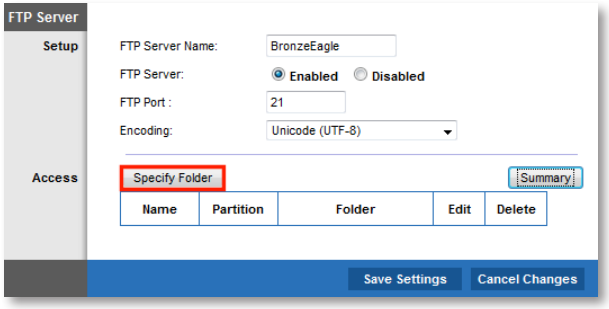
How to share folders and set access rights

You can select which folders to share. You can also select which users can access the folders. For more information on managing access rights, see "How to configure storage" on page 32.

To configure FTP and control folder access:

Storage > FTP Server

1. In the *Storage* tab's *FTP Server* page, click **Specify Folder**.



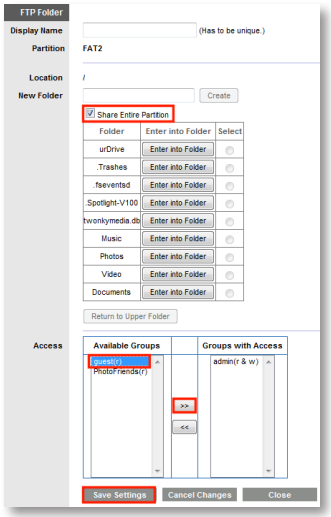
The *FTP Folder* screen opens in a separate window.

2. In the **Display Name** field, enter a unique name for the FTP folder. The name must use only alphanumeric characters (letters A to Z and numbers 0 to 9) and can be up to 15 characters long.
3. To share the entire drive, click **Share Entire Partition**.

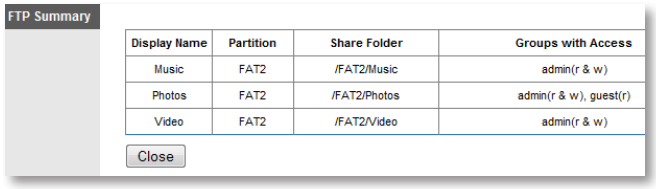
   – OR -

   To share only specific folders:

   - Click **Select** next to the folder you want to share.
   - To navigate to a previous folder, click **Return to Upper Folder**.
   - To view and select folders within a folder, click **Enter into Folder** next to the folder name.
4. To create a folder, enter a unique folder name into the **New Folder** box, then click **Create**.
5. To change group access, select a group in the *Available Groups* or *Groups with Access* column, then click >> or << to move the group to the other column.
6. To apply your changes and enable FTP access, click **Save Settings**.



7. To apply your changes and create the shared folder for FTP access, click **Save Settings**. You are returned to the *FTP Server* page, where a summary of shared folders is displayed.
8. To modify shared folder settings:
   - To change a FTP folder's name or group access, click **Edit**.
   - To delete an FTP folder, click **Delete**.
   - To see a detailed summary of FTP folders, click **Summary**. A separate window opens and shows the folder's *Display Name*, *Partition*, *Share Folder*, and *Groups with Access*. Click **Close** to close the window.



How to access files remotely

To access files remotely, you must first attach a USB drive to your router and set up that storage for remote access. For instructions, see "How to configure your router's storage for remote access" on page 36. You can then access files from anywhere on the Internet.

To access files remotely:

1. Make sure that your router is configured to share files. For more information, see "How to configure your router's storage for remote access" on page 36.
2. Make sure that your router has user accounts set up, and that you have taken note of the user name and password you will use to access the router's storage. If you have enabled Anonymous FTP (not recommended), you will not need a user name and password. For more information, see "How to configure storage" on page 32.
3. Take note of the IP address of your router. To view your router's IP address, open the browser-based utility, click the **Status** tab, then click the **Router** page and take note of the numbers in the *Internet IP Address* field.

   – OR –

   If you have *DDNS* (Dynamic Domain Name Service), take note of the domain name registered to your router. For more information, see "How to find your network on the Internet" on page 16.
4. At any remote location where you can access the Internet, you can:
   - Use FTP (File Transfer Protocol) client software to connect to your router. You will need to enter your router's IP address. If access to your router requires a user name and password, you will also need to enter those details. For more information on using the FTP client software, see its documentation or help.

     – OR –
   - Type the router's IP address into a web browser's Internet address field, press **Enter**, then enter your user name and password.

FTP software and web browsers display FTP content in many ways, but you can usually use these common actions to navigate through FTP folders:

- Click a folder name to open it.
- Click a double period (..) or **Up to a higher level directory** to open a parent folder.
- Click or right-click a file to download or view it.
- Drag a file from another window and drop it into the FTP window to upload it. (To upload a file, your user account must have write access.)

Port Forwarding and Port Triggering

How to set up port forwarding

Why would I use port forwarding? Port forwarding is a feature that forwards inbound traffic from the Internet on a specific port or ports to a specific device or port on your local network. You can set up port forwarding for:

- A single port (see "How to set up port forwarding for a single port" below)
- Multiple ports (see "How to set up port forwarding for multiple ports" on page 40)
- A range of ports (see "How to set up port forwarding for a range of ports" on page 40)

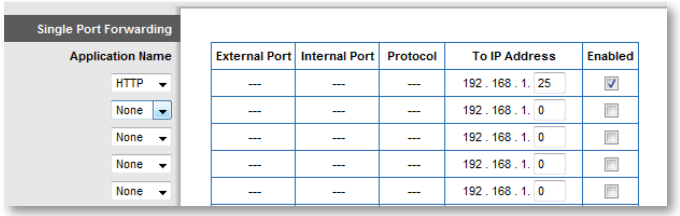
How to set up port forwarding for a single port

Why would I use port forwarding for a single port? Single port forwarding is a feature that forwards inbound traffic from the Internet on a specific port to a single device on your local network. An example of single port forwarding would be to forward inbound web requests, typically on port 80, to a web server.

To set up single port forwarding:

Applications & Gaming > Single Port Forwarding

1. Follow your device's instructions for configuring it with a static IP address or use DHCP reservation to assign it a permanent address (see "How to set up the DHCP server on your router" on page 15).
2. Log into the browser-based utility (see "How to open the browser-based utility" on page 14).
3. Click the **Applications & Gaming** tab, then click the **Single Port Forwarding** page.



4. Select the type of application from the **Application Name** drop-down list. One of the more common types to select is **HTTP**, but see your device's documentation for recommendations.
5. In the **To IP Address** field, enter the last three digits of the IP address you have reserved for the computer you want to forward Internet traffic to. The rest of the IP address has already been completed for you.
6. Select **Enabled** next to the *IP Address field*.
7. Click **Save Changes** at the bottom of the screen.

TIP

For other devices not included in the Application Name drop-down list, see the device's documentation for port and protocol information.

How to set up port forwarding for multiple ports

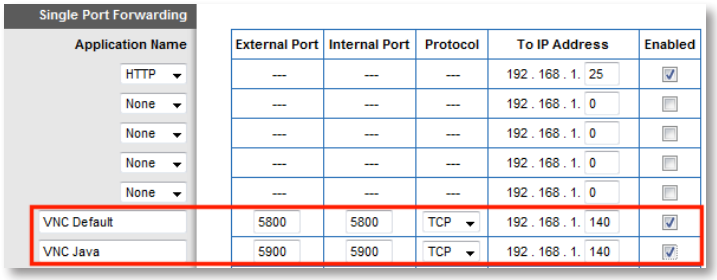
Why would I set up port forwarding for multiple ports? Port forwarding is a feature that forwards inbound traffic from the Internet on a specific port to a single device on your local network. Unlike a web camera that typically only requires a single port to be forwarded, some applications require forwarding of multiple ports. *VNC* (Virtual Network Computing) software that allows you to operate your computer remotely from anywhere on the Internet is an example of an application that requires multiple ports to be forwarded. To forward to multiple ports, just create additional entries to forward additional ports to the same IP address.

Example: You want to set up your computer so you can remotely access it using VNC software. By default, VNC uses TCP ports 5800 and 5900.

To set up single port forwarding for multiple ports:

Applications & Gaming > Single Port Forwarding

1. Make sure that the software you want to use has been installed onto a networked computer.
2. Log into the browser-based utility (see "How to open the browser-based utility" on page 14).
3. Set up DHCP reservation for the IP address of the computer on which you installed the software. (See "How to set up the DHCP server on your router" on page 15).
4. Click the **Applications & Gaming** tab, then click the **Single Port Forwarding** page.
5. For each entry, enter a descriptive name in the **Application Name** field.
6. For each entry, enter in the same port number for the **External Port** and the **Internal Port**.
7. In the **To IP Address** field, enter the last three digits of the IP address you have reserved for the computer you want to forward Internet traffic to. The rest of the IP address has already been completed for you.
8. Select **Enabled** next to the *IP Address* field.



9. Click **Save Changes** at the bottom of the screen.

NOTE

If you want to use software such as VNC on multiple computers, you will need to reconfigure the default ports that VNC uses on each additional computer. Then, create additional port forwarding entries for each additional computer. See your software's documentation for help.

How to set up port forwarding for a range of ports

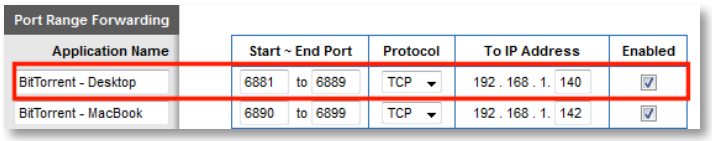
Why would I set up port forwarding for a range of ports? Port forwarding is a feature that forwards inbound traffic from the Internet on a range of ports to a single device on your local network. Unlike a web camera that typically only requires a single port to be forwarded, some applications require forwarding to a range of ports.

Example: You want to set up your computer so you can use BitTorrent, a popular peer-to-peer file sharing application. BitTorrent uses port 6881 by default. If that port is busy, the requesting BitTorrent client tries the next port in sequence. The most common configuration for home routers with a single BitTorrent computer is to set up port forwarding using a range of ports starting with 6881 and ending with port 6889.

To set up port range forwarding:

Applications & Gaming > Port Range Forwarding

1. Log into the browser-based utility (see "How to open the browser-based utility" on page 14).
2. Set up a DHCP reservation for the IP address of the computer on which you installed the software. (See "How to set up the DHCP server on your router" on page 15). In this example, the IP address of the desktop computer with BitTorrent installed is 192.168.1.140.
3. Click the **Applications & Gaming** tab, then click the **Port Range Forwarding** page.
4. Enter a descriptive name, then enter the **Start Port** and the **End Port** values to specify the range. In this example, the range is 6881 to 6889.
5. Select **TCP** as the protocol.
6. In the **To IP Address** field, enter the last 3 digits of the IP address of the device running the software. The rest of the IP address fields already completed. In this example, you would enter 140.
7. Select **Enabled** next to the *To IP Address* field.



8. Click **Save Settings** at the bottom of the page.

NOTES:

To use software like BitTorrent on multiple computers on your network, create additional entries with a unique range of ports as shown above. BitTorrent only works with ports between 6881 and 6999.

Depending on your computer's firewall software, you may need to open a range of ports in your firewall to enable software that uses port range forwarding

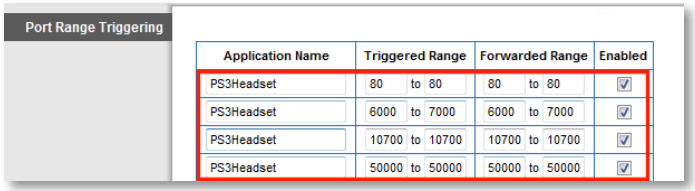
How to set up port range triggering for online gaming

Why would I use port triggering instead of port forwarding? Port range triggering allows the router to watch outgoing data for specific port numbers. The IP address of the computer that sends the matching data is remembered by the router, so that when the requested data returns through the router, the data is routed back to the proper computer. An example of port range triggering would be to enable a USB or Bluetooth headset for online chat and gaming.

To set up port range triggering for multiple entries:

Applications & Gaming > Port Range Triggering

1. Log into the browser-based utility (see "How to open the browser-based utility" on page 14).
2. Click the **Applications & Gaming** tab, then click the **Port Range Triggering** page.
3. See your device documentation for information on the ports that the device uses.
4. For each entry in the *Port Range Forwarding* table:
   - Enter a descriptive name (such as *PS3 Headset*)
   - For single ports, enter the same port number in each **Triggered Range** and **Forwarded Range** box.
   - For port ranges, enter the same number ranges in each **Triggered Range** and **Forwarded Range** column.



5. Click **Save Settings** at the bottom of the page.

How to configure your Xbox for online gaming

Why would I set up my Xbox for online gaming? Online gaming adds another dimension to using your Xbox. As with other online gaming applications and gaming consoles, you need to forward multiple ports to use your Xbox for online gaming. The procedure for setting up your Xbox is almost identical to setting up multiple port forwarding for VNC remote control. (See "How to set up port forwarding for multiple ports" on page 40).

> **NOTE**
> For more information on configuring your router for online gaming, see "How to optimize your router for gaming and voice" on page 19.

Refer to your game console documentation to determine the ports used by your device. The Xbox uses four ports:

- TCP port 80
- UDP port 88
- TCP/UDP port 53
- TCP/UDP port 3074

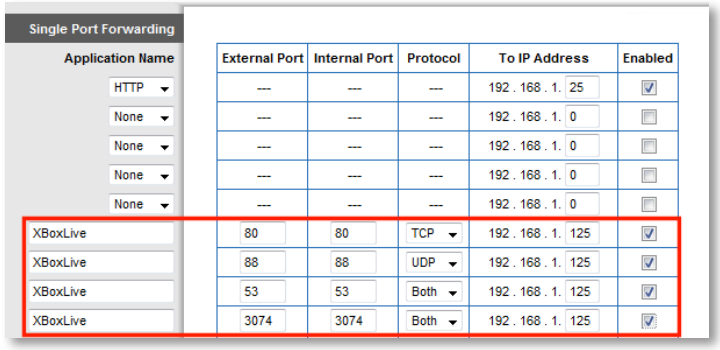
To set up an Xbox using multiple entries of single port forwarding:

Applications & Gaming > Single Port Forwarding

1. Connect your Xbox 360 to your router.
1. Log into the browser-based utility (see "How to open the browser-based utility" on page 14).
2. Set up a DHCP reservation for the IP address of the Xbox. (See "How to set up the DHCP server on your router" on page 15).

   – OR –

   Refer to your game console's documentation to set a static IP address for your device.
3. Click the **Applications & Gaming** tab, then click the **Single Port Forwarding** page. The Xbox uses four ports, so create four port forwarding entries on this page.
4. Enter the port and protocol information as shown in the image below.



5. In the **To IP Address** field, enter a 1- to 3-digit number that corresponds to the last three digits of the IP Address of the Xbox 360. The rest of the IP address is already completed.
6. Select **Enabled** next to the *To IP Address* field for each entry.
7. Click **Save Settings** at the bottom of the page.

Maintaining and Monitoring

How to back up and restore your router configuration

Why do I need to back up my router configuration? As with any valuable data, you should back up your router configuration. Your router might contain many customized settings. Those settings would be lost if you reset your router to its factory defaults, and you would need to re-enter all of them manually. If you back up your router configuration, restoring settings is easy.

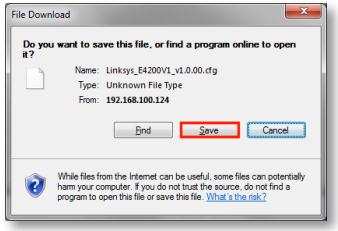
To back up your router configuration:

Administration > Management

1. Log into the browser-based utility (see "How to open the browser-based utility" on page 14).
2. Click the **Administration** tab, then click the **Management** page.
3. Click **Back Up Configurations** at the bottom of the screen.

You are prompted to save the file.

4. Click **OK** or **Save**.

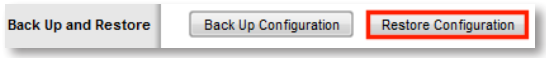


5. Specify a file location, then click **Save**.

To restore your router configuration:

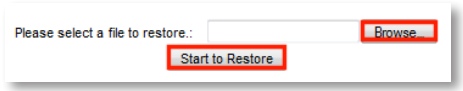
Administration > Management

1. Log into the browser-based utility (see "How to open the browser-based utility" on page 14).
2. Click the **Administration** tab, then click the **Management** page.
3. Click **Restore Configurations** at the bottom of the screen.



A separate window opens.

4. Click **Browse** to navigate to the location of your configuration file, then select the file and click **Open**.
5. To restore the configuration, click **Start to Restore**.



How to restore factory defaults

Why would I need to restore to factory defaults? If you are experiencing difficulties with the router and have exhausted all other troubleshooting measures, you may want to reset the router to factory defaults. Resetting the router erases all of your settings, so you must restore the settings after. We recommend that you back up your configuration before resetting your router to factory defaults. See "How to back up and restore your router configuration" on page 43.

You can use the Reset button or the router's browser-based utility to restore your router to factory defaults.

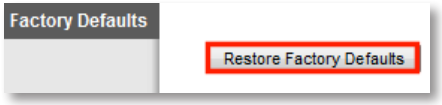
To reset your router to factory defaults with the reset button:

1. With your router connected to power and turned on, press and hold the **Reset** button on the bottom of your router for 5-10 seconds.

To reset your router to factory defaults using the browser-based utility:

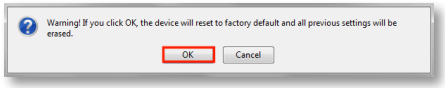
Administration > Factory Defaults

1. Log into the browser-based utility (see "How to open the browser-based utility" on page 14).
2. Click the **Administration** tab, then click the **Factory Defaults** page.
3. Click **Restore Factory Defaults**.



A confirmation window opens.

4. Click **OK**.



How to upgrade the router's firmware

Why would I need to upgrade my router's firmware? Linksys may periodically publish a firmware upgrade either to fix a problem or to add features to your router.

IMPORTANT

Do not interrupt the upgrade process. You should not turn off the router or press the Reset button during the upgrade. Doing so may permanently disable the router.

If you are upgrading from a laptop computer, make sure that the laptop is connected to a power source or that the battery is fully charged.

Disable your computer's Sleep mode. It might interrupt the upgrade process.

If you are upgrading from a computer with a wireless network connection, make sure that you have strong wireless signal strength. If not, move your computer closer to your router.

TIPS

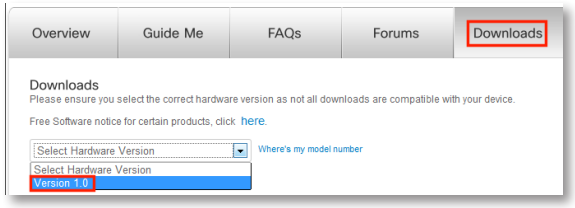
Each time you run Cisco Connect, it checks for software updates and installs them, if available. Use the following instructions only if you don't run Cisco Connect.

To upgrade the router's firmware:

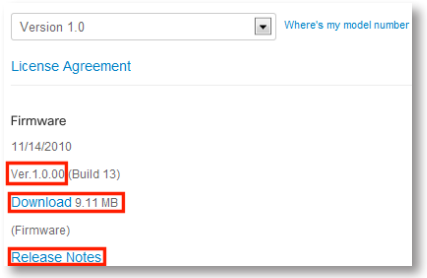
Linksys.com/support
Administration > Firmware Upgrade

1. Log into the browser-based utility (see "How to open the browser-based utility" on page 14).
2. Click the **Status** tab, then click the **Router** page and take note of the current firmware version for your router.
3. Using your web browser, connect to **Linksys.com/support**, then find your router model.

4. Click the **Downloads** tab, then select the hardware version for your router from the **Select Hardware Version** drop-down list.

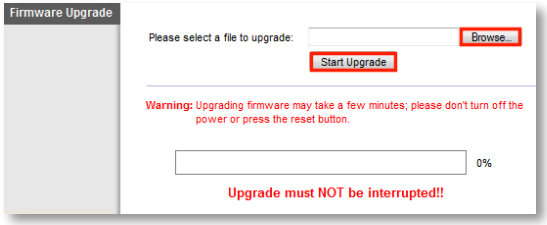


5. Compare the latest available firmware version on the website with your current version. If there is a newer version, click **Release Notes** to see if the newer version contains new features you want or solves a problem you are having.
6. If you want the new version, click **Download** and save the file to your computer. Take note of the file location.



During the upgrade process, the router may lose the settings you have changed. Make a backup of your router configuration *before* starting the upgrade process. See "How to back up and restore your router configuration" on page 43.

7. In the browser-based utility, click the **Administration** tab, then click the **Firmware Upgrade** page.
8. Click **Browse**, then go to the location where you saved the upgrade file.
9. Select the upgrade file, then click **Start Upgrade** and follow the on-screen instructions. The upgrade process begins, and a progress bar appears. When the firmware has been uploaded, a new page opens with an "Upgrade is successful" notice, and the router reboots.



How to check the status of your router

Why would I want to check the status of my router? Your router status tells you whether you have a secure Internet connection and informs you about the status of your network-connected devices.

To check your router status using Cisco Connect:

1. In Windows, click **Start**, **All Programs**, then click **Cisco Connect**.

   – OR –

   On a Mac, open the **Applications** folder, then click **Cisco Connect**.

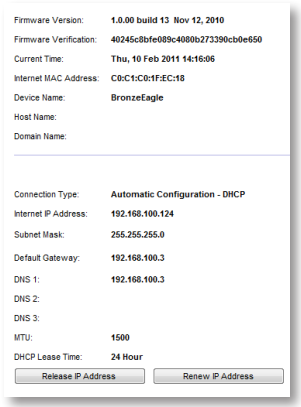
   The Cisco Connect main menu opens.
2. Look in the upper-right corner of the Cisco Connect main menu. If your router is online and secure, you see *online secure* and a green indicator.

To check your router status using the browser-based utility:

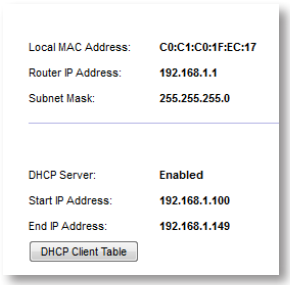
Status > Router
Status > Local Network
Status > Wireless Network
Status > Ports

1. Log into the browser-based utility (see "How to open the browser-based utility" on page 14).
2. Click the **Status** tab, then click the **Router** page. Detailed information about your router status is displayed.

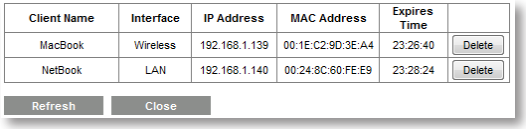
TIP
For field descriptions, click **Help** on the right side of the screen.



3. Click the **Status** tab, then click the **Local Network** page. Your local network's IP address information and the DHCP server settings are displayed.



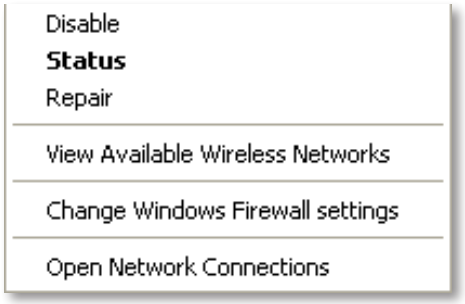
4. Click **DHCP Client Table** to display the currently assigned IP addresses.



Client Name	Interface	IP Address	MAC Address	Expires Time	
MacBook	Wireless	192.168.1.139	00:1E:C2:9D:3E:A4	23:26:40	Delete
NetBook	LAN	192.168.1.140	00:24:8C:60:FE:E9	23:28:24	Delete

Refresh Close

5. Click the **Status** tab, then click the **Wireless Network** page. Your wireless network status is displayed.



6. Click the **Status** tab, then click the **Ports** page. The link status and speed (speed data available only for the E3200 and E4200) for each of the Ethernet ports and the Internet port are displayed.

How to disable the Ethernet port status lights

Why would I want to disable the Ethernet port status lights? Depending on the placement of the router in a home, some users might find the lights distracting. You can easily disable the lights using Cisco Connect, but you can also disable them using the browser-based utility.

To disable the lights using Cisco Connect:

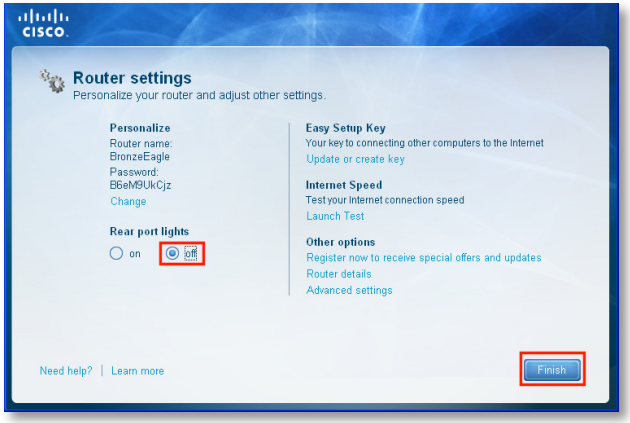
1. In Windows, click **Start**, **All Programs**, then click **Cisco Connect**.

   – OR –

   On a Mac, open the **Applications** folder, then click **Cisco Connect**.

   The Cisco Connect main menu opens.

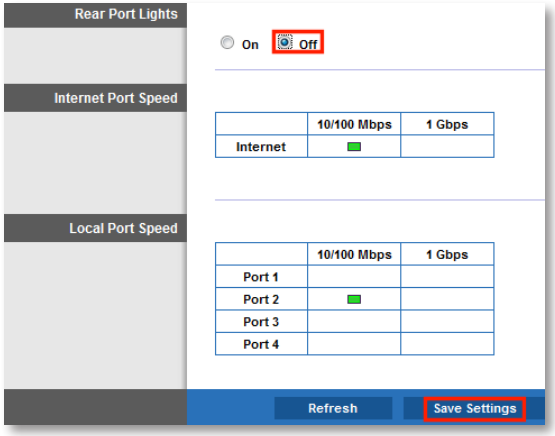
2. Under *Router Settings*, click **Change**.
3. Under *Port lights*, click **Off**, then click **Finish**.



To disable the lights using the browser-based utility:

Status > Ports

1. Log into the browser-based utility (see "How to open the browser-based utility" on page 14).
2. Click the **Status** tab, then click the **Ports** page.
3. In the *Rear Port Lights* section, click **Off**, then click **Save Settings**.



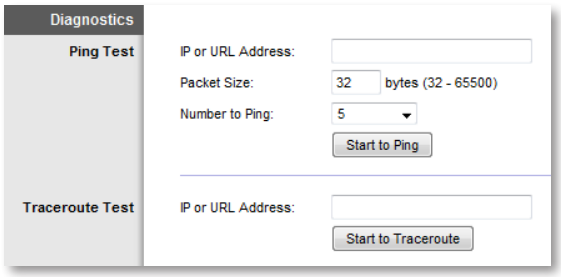
How to test your Internet connection

What utilities are included in my router to test my Internet connection?
Your router includes two diagnostic tests, Ping and Traceroute, that let you check network connections, including network devices and your Internet connection.

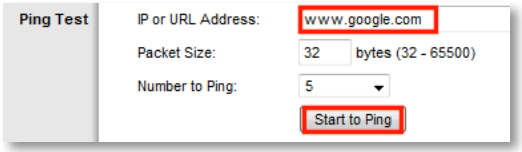
To diagnose your Internet connection:

Administration > Diagnostics

1. Log into the browser-based utility (see "How to open the browser-based utility" on page 14).
2. Click the **Administration** tab, then click the **Diagnostics** page.

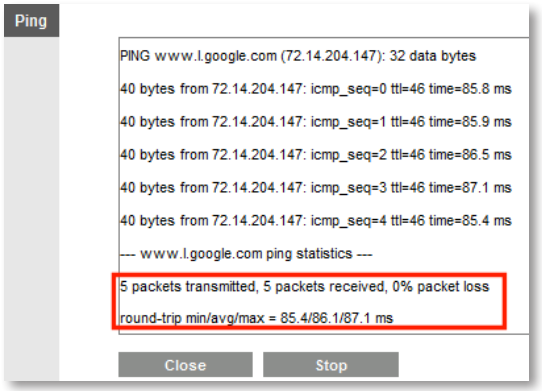


3. To check whether an address can be reached, enter an IP address or URL, a packet size, and number of times to ping in the *Ping Test* section, then click **Start to Ping**.

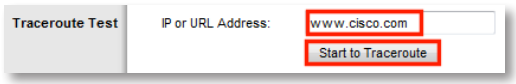


A window opens showing the ping test results. You will see a response for each successful ping.

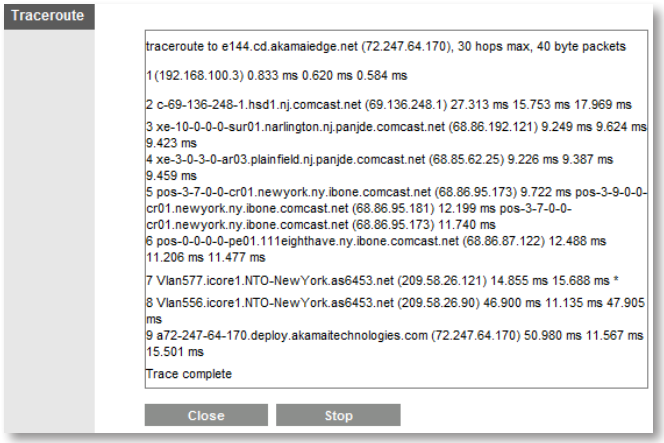
NOTE
If an Internet URL fails to respond to ping, it doesn't necessarily mean that the site is down. For security reasons, some sites are configured to not respond to ping requests.



4. To trace the route that packets take between your router and a specific address, enter an address in the **IP** or **URL Address** field of the *Traceroute Test* section, then click **Start to Traceroute**.



A window opens with the test results.



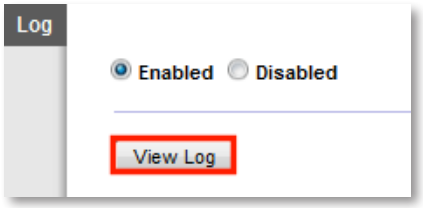
How to configure and use logs

What kind of logging capabilities does my router have? Your router can track all traffic for your Internet connection. Your router supports four types of logs:

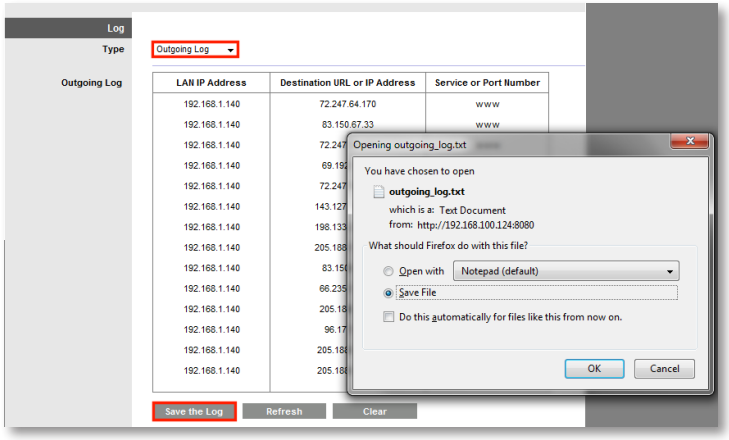
To enable and view router logs:

Administration > Log

1. Log into the browser-based utility (see "How to open the browser-based utility" on page 14).
2. Click the **Administration** tab, then click the **Log** page.
3. To monitor traffic between the local network and the Internet, select **Enabled** (default), then click **Save Settings**.
4. To view the logs, click **View Log**. The *Log* window opens.



5. Select the log you want to see from the **Type** drop-down list.



- **Incoming Log**—The source IP addresses and destination port numbers for incoming Internet traffic
- **Outgoing Log**—Local IP addresses, destination URLs/IP addresses, and service/port numbers for outgoing Internet traffic
- **Security Log**—Logins for the browser-based utility
- **DHCP Client Log**—Local DHCP server status information

6. To save the log, click **Save the Log**, then click **OK** or **Save**.

Specifications

Linksys E1550

Model Name	Linksys E1550
Description	Wireless-N Router with SpeedBoost
Model Number	E1550
Standards	802.11n, 802.11g, 802.11b, 802.3u
Ports	Power, Internet, Ethernet (1-4), USB
Buttons	Reset, Wi-Fi Protected Setup
LEDs	Power/Wi-Fi Protected Setup, Internet, Ethernet (1-4)
Cabling Type	CAT 5e
Transmitted Power	802.11b: 16.5 ± 1.5 dBm 802.11g: 14.5 ± 1.5 dBm 802.11n: (20 MHz): 15.0 ± 1.5 dBm @Ch. 6, MCS0, 8 (20 MHz): 13.5 ± 1.5 dBm @Ch. 6, MCS7, 15 (40 MHz): 13.5 ± 1.5 dBm @Ch. 6, MCS0, 7, 8, 15
Antenna Gain	Antenna 1: ≤ 2.5 dBi Antenna 2: ≤ 3 dBi Antenna 3 ≤ 4 dBi
Receive Sensitivity	802.11b: -87 dBm @ 11 Mbps (Typ.) 802.11g: -71 dBm @ 54 Mbps (Typ.) 802.11n (20 MHz): -69 dBm @ MCS15 (Typ.) 802.11n (40 MHz): -66 dBm @ MCS15 (Typ.)
UPnP	Supported
Wireless Security	WEP, WPA, WPA2
Security Key Bits	Up to 128-Bit Encryption

Environmental

Dimensions	7.95" x 1.34" x 6.3" (202 x 34 x 160 mm)
Unit Weight	9.81 oz (280 g)
Power	12V, 1.5A
Certifications	FCC, CE, ICES-003, Wi-Fi (802.11b/g/n), UL/cUL, Windows 7
Operating Temp.	32 to 104°F (0 to 40°C)
Storage Temp.	-4 to 140°F (-20 to 60°C)
Operating Humidity	10 to 80% Noncondensing
Storage Humidity	5 to 90% Noncondensing

Specifications are subject to change without notice.

Browser-based Utility Menu Structure

Linksys E1550

- **Setup**
  - Basic Setup
    - Language
    - Internet Setup
      - Internet Connection Type
      - Optional Settings
    - Network Setup
      - Router Address
      - DHCP Server Setting
    - Time Settings
      - Time Zone
    - Reboot
  - DDNS
    - DDNS
      - DDNS Service
  - MAC Address Clone
    - MAC Address Clone
  - Advanced Routing
    - NAT
    - Dynamic Routing (RIP)
    - Static Routing
- **Wireless**
  - Basic Wireless Settings
    - Configuration View
  - Wireless Security
    - Wireless Security
  - Guest Access
    - Guest Access
  - Wireless MAC Filter
    - Wireless MAC Filter
      - Access Restriction
      - MAC Address Filter List
- **Security**
  - Firewall
    - Firewall
    - Internet Filter
    - Web Filter
  - VPN Passthrough
    - VPN Passthrough
- **Storage**
  - Disk
    - Disk Management
      - Shared Folder
      - Format Disk
  - FTP Server
    - Setup
    - Access
  - Administration
    - Information
    - Anonymous Access
    - User Management
    - Group Management
- **Access Policy**
  - Parental Controls
    - Target Devices
    - Schedule
    - Block Specific Sites
- **Applications & Gaming**
  - Single Port Forwarding
    - Single Port Forwarding
      - Application Name
  - Port Range Forwarding
    - Port Range Forwarding
      - Application Name
  - Port Range Triggering
    - Port Range Triggering
  - DMZ
    - DMZ
  - QoS
    - QoS (Quality of Service)
      - Wireless
      - Internet Access Priority
      - Upstream Bandwidth
      - Category
      - Summary
- **Administration**
  - Management
    - Router Access
    - Local Management Access
    - Remote Management Access
    - Advanced features
    - UPnP
    - Back up and Restore
  - Log
    - Log
  - Diagnostics
    - Diagnostics
      - Ping Test
      - Traceroute Test
  - Factory Defaults
    - Factory Defaults
  - Firmware Upgrade
    - Firmware Upgrade
- **Status**
  - Router
    - Router Information
    - Internet Connection
  - Local Network
    - Local Network
    - DHCP Server
  - Wireless Network
    - Wireless Network
  - Ports
    - Rear Port Lights
    - Internet Port Link
    - Local Port Link

Visit **linksys.com/support** for award-winning 24/7 technical support

3425-00977